Discord Exploitation Lab

Hacking-Lab for Discord bots inspired by the OWASP Top Ten

Students

Dante Suwanda

Janosch Bühler

Initial Situation: Discord is an instant messaging and VoIP based platform, popular in gaming, tech and communities of all kind. Servers created by users can have their functionalities extended and automated by community-made bots.
These bots, while useful, can be vulnerable to issues like injection flaws and broken authentication, aligning with the vulnerabilities described in the newest OWASP Top Ten.
There's a noticeable lack of practical, interactive training for securing Discord bots, even though there's plenty of theoretical information available. This highlights the need for hands-on learning experiences to effectively understand and address these vulnerabilities.

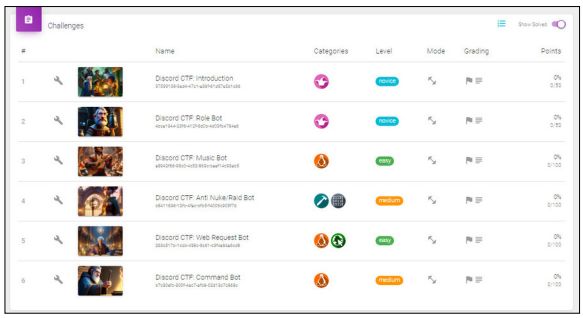
Approach / Technology: Our goal was not only to create an educational lab about Discord bot security, but also to present it in a playful and game-like manner. As a result we have created several vulnerable Discord bots with built-in vulnerabilities and provide them as so-called Hacking-Lab challenges.
The aim was to make solving challenges enjoyable, resembling a role-playing game where students walk through an adventure, encountering five different characters represented by Discord bots, each with their own vulnerability and challenge.
For the development of this lab we used Python in combination with the Nextcord library to develop our insecure bots and Docker Compose for instance management, within the Hacking-Lab framework.

Result: In total 5 different Hacking-Lab challenges were implemented. The challenges are included in OST's Hacking-Lab and highly inspired by OWASP Top Ten. The challenges can be solved on their own, but in our lab, we've integrated each bot into a bigger story to make the journey more interesting.

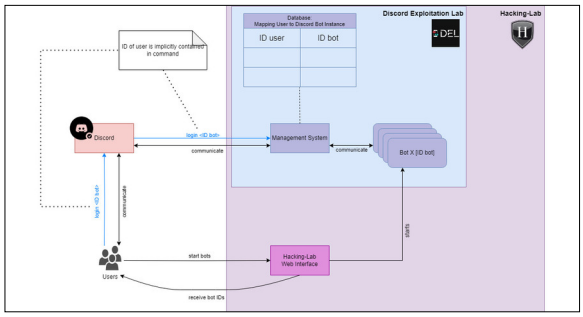
We developed two distinct types of bots: one operates as a straightforward Discord bot, engaging directly with users, while the other is more complex, generating an instance for each user. This latter type is crucial in challenges where users might potentially gain full access to the bot's operating system, thus posing a threat to its integrity. To safeguard the lab experience for concurrent users and prevent any interference, we engineered this specific bot type.

DEL - Discord Exploitation Lab Logo
Own presentment

Hacking-Lab Page - Challenges O
Own presentment



Framework Structure for Pseudo Bots of the DEL Hacking-Lab
Own presentment



Advisor
Ivan Bütler

Subject Area
Networks, Security & Cloud Infrastructure, Software

Project Partner
Compass Security and Hacking-Lab AG, Jona, St.Gallen