Bug Bounty Hunting and Reconnaissance at GenCyberCoin

A Sample Lesson Plan

Lesson Description

Students will learn about different attack vectors on websites (Bug Bounty) as well as Social Engineering and Reconnaissance (Open Source Intelligence Gathering, OSINT). By following the Bug Bounty hints, they will be able to discover a variety of client- and server-side bugs and automatically get rewarded with GenCyberCoins for those. The bugs include: sensitive data exposure, broken authentication, XSS, user input validation, local file inclusion, and others. Additionally, students will engage in OSINT activities by answering the questions that we developed and added on the GenCyberCoin platform.

Prerequisite Knowledge

Students should have a basic understanding of how to use a web browser and look for information in a search engine.

Length of Completion

Typically, the lesson is completed in ~90-120 minutes.

Level of Instruction

The lesson is intended for high school learners at the beginner and intermediate levels.

Applicable First Principles &/or Concepts

GenCyber First Principles

Domain Separation	**Abstraction**
Process Isolation	**Data Hiding**
Resource Encapsulation	**Layering**
Modularity	**Simplicity**
Least Privilege	Minimization

GenCyber Cybersecurity Concepts

Defense in Depth	Availability
Confidentiality	**Think like an Adversary**
Integrity	**Keep it Simple**

Resources that are Needed

1. A laptop, PC, or a Raspberry Pi setup
2. Browser
3. Information is available at https://github.com/vitalyford/gencybercoin

Accommodations Needed

Special technical setup may be needed for students who are visually or physically impaired to use the computer.

LESSON LEARNING OUTCOMES

- Demonstrate the ability to think out of the box and identify what can go wrong on a website (but bounty feature).
- Demonstrate the ability to use a search engine to find the necessary information during the Reconnaissance phase (reconnaissance feature).
- Learn about different types of vulnerabilities that are typical for websites (bug bounty feature).
- Learn the basics of web ethical hacking and exploitation (but bounty feature).

LESSON DETAILS

Assessment

The assessment for this lesson is a combination of walk-around observation and statistics of the following:

1. The number of students answering the Reconnaissance questions correctly (the OSINT Ninjas page).
2. The results of the Bug Bounty activity (the Hall of Fame page).

Extension Activities on the GenCyberCoin platform

- Learn about password strength, where to check if the email and password have been compromised, and how to correctly manage it.
- Learn about digital currency.
- Learn about blockchain and its applications beyond cryptocurrency.

Differentiated Learning Opportunities

Advanced students can find more bugs within the allocated time and learn more by exploring the links that are related to the found bugs. Also, advanced students can discover more sophisticated search queries by spending more time reading the material provided in the Reconnaissance activity.

LESSON

Preparation

The instructor can learn herself how the platform works by watching a 12-minute video on https://github.com/vitalyford/gencybercoin. Next, the instructor needs to follow the directions for deploying on Heroku. After the system is deployed, the instructor logs in with "gcsuperuser/gcsuperuser" credentials, changes the password, and shares the URL of the deployed platform with her students. She can also create a code for her teaching assistants or herself to be admins for the school if they would like to change anything on the market or create new badges and activity information.

Student information

The instructor can show a 2-minute video about the GenCyberCoin platform to the students: https://github.com/vitalyford/gencybercoin

Students navigate to the shared URL and register on the platform, selecting "Trial" at the very bottom of the registration page.

Sample lesson plan

1. Register an account and explore the GenCyberCoin platform.
2. Navigate to Features → Bug Bounty to learn about what kinds of bugs to search for on the platform. There are hints in place to help you find those bugs.
3. Navigate to Features → Reconnaissance to learn about Open Source Intelligence Gathering (OSINT) and Social Engineering.
4. Answer as many questions as you can on the Reconnaissance page. Everybody can see everyone's progress on the OSINT Ninjas page.
5. Find as many bugs as you can on the Bug Bounty page. Everybody can see everyone's progress on the Hall of Fame page.
6. As you progress through the activities, you automatically earn GenCyberCoins and every action/transaction is tracked on the Blockchain (Features → Blockchain).
7. Discuss the details of Reconnaissance and Bug Bounty as well as their implications in the real world.

Questions/Concerns/Suggestions/Bugs

Please reach out to Vitaly Ford at fordv@arcadia.edu