The 21st World Conference on Information Security Applications

WISA 2020

August 26-28, 2020

MAISON GLAD, Jeju Island, Korea

Hosted by
Korea Institute of Information Security & Cryptology

Sponsored by
Ministry of Science and ICT
NIS

Co-Sponsored by
KIS, ETRI, KONA International, WINS
Toward a Fine-Grained Evaluation of The Pwnable CTF: Extracting Common Assessment Points*

Sung-Kyung Kim\textsuperscript{1}[0000--0003--2782--271X], Eun-Tae Jang\textsuperscript{1}[0000--0002--7368--551X], and Ki-Woong Park\textsuperscript{1}[0000--0002--3377--223X]

Department of Information Security, Sejong University, Seoul, South Korea
{\texttt{jotun9935, euntaejang}@gmail.com, woongbak@sejong.ac.kr}

Abstract. Capture the Flag (CTF) is recognized for its high educational value as it allows students to actively practice techniques for bypassing security systems. Accordingly, some research has attempted to increase the learning efficiency of participants and ease the burden of educators in the operation of CTF. However, in the pwnable field, which is one of the representative fields of CTF, high entry barriers exist for participants because it requires a comprehensive understanding of program analysis, attack and defense techniques, and systems. Therefore, educators require to introduce an education method to lower the pwnable entry barrier for learners. However, when educators introduce CTF-style pwnable education in the classroom, the more students and the more questions that require complex knowledge, the more the educator must pay for analysis of the learner’s failure factors. Therefore, new methods are needed to reduce these costs. To address this necessity, this paper is a preliminary study of the CTF platform to enable automated analysis of the causes of learners' failures by instituting detailed evaluation points for common pwnable problems.

Keywords: Capture the Flag · CTF · Pwnable · Memory Corruption Exploit

1 Introduction

Recently, because the effectiveness of learning via practice has been confirmed experimentally\cite{3, 14, 16}, education using Capture the Flag (CTF) in information security education is emerging as a new paradigm. In accordance with this paradigm, research and education platforms for information security educators to improve accessibility for beginners are being developed\cite{4, 7, 5, 15, 2, 16}. However, the implementation of CTF is a burden on time and finances for educators. In recent years, new techniques, such as automated problem creation, have been applied to reduce the burden of CTF application\cite{1, 8, 1, 7}. However, it is important to analyze the failure factors of learners through precise scoring and

* Supported by the Institute for Information Communications Technology Promotion (IITP) of the Korea government (MSIT) [Grant No. 2018-0-00420, 2019-0-00273]
evaluation, as well as creating effective problems in the operation of CTF. This is because educators can improve the student’s learning efficiency by showing the student’s weaknesses in the problem-solving process through provision of clear feedback and active support to improve themselves[14]. However, as shown in Fig. 1, the evaluation method used in many existing CTFs is that when the solver submits a flag to the scoring server, which is obtained when the problem is completely solved, the solver is evaluated in a pass and/or non-pass manner. In this scoring method, it is difficult to identify the learner’s point of failure. Hence, educators must invest additional time and economic costs to analyze the cause of the learner’s failure. For a CTF, pwnables, which require a comprehensive understanding of binary and system knowledge and exploitation techniques, have particularly high costs. Pwnable problems generally necessitate knowledge of development, systems, attack defense technique, program analysis technology, etc. For example, memory corruption exploitation, a type that is commonly presented in the pwnable field, consists of a process that triggers vulnerabilities in the program by entering invalid input and then hijacking the program’s control flow by bypassing the present in the system. Thus, learners need a comprehensive understanding goals of all processes to solve problems in the pwnable field (see Table 1). That is, if a learner fails at any point, it results in a total failure. Therefore, this paper is the first attempt at designing a pwnable platform that enables precise feedback automation on learner failure factors and aims to derive