Automated Vulnerability Assessment for Web APIs Employing Response Data

Yuki Ishida[*], Masaki Hanada[**], Atsushi Waseda[**], and Moo Wan Kim[***]

[*] Graduate School of Informatics, Tokyo University of Information Sciences, Japan

[**] Department of Informatics, Tokyo University of Information Sciences, Japan

[***] TA Tech., Japan

h22001iy@edu.tuis.ac.jp, mhanada@rsch.tuis.ac.jp, aw207189@rsch.tuis.ac.jp, ykim5jp@ybb.ne.jp

***Abstract*— In recent years, Web Application Programming Interfaces (Web APIs) have been extensively used in numerous web applications. However, the number of attacks exploiting Web API vulnerabilities has been rapidly increasing. The Open Web Application Security Project (OWASP) published guidelines known as the OWASP API Security Top 10 to mitigate the risks associated with these vulnerabilities. The guidelines identify the top 10 most critical security risks in Web APIs and provide remediation guidance to help developers. Although developers are required to address these vulnerabilities according to these guidelines, traditional vulnerability assessment tools may not perform adequately when used to assess Web API vulnerabilities. Manually addressing these is difficult because there are a large number of endpoints and parameters in Web APIs using traditional vulnerability assessment tools. To address this issue, we propose a method for automatically conducting Web API vulnerability assessments by utilizing references, requests, and responses for Web APIs. In the evaluation experiment, we showed that the proposed method can detect authorization-related vulnerabilities in the Web APIs of vulnerable testing environments and well-known Content Management Systems, such as Wordpress, Ghost CMS, and Joomla.**

***Keywords*— Web API, Vulnerability Assessment, Automation Analysis, Security**

Yuki Ishida was born in Japan 1991, received the B.E. and M.S. degrees in Informatics from Tokyo University of Information Sciences, Japan, in 2014 and 2016, respectively. Upon graduation in 2016, he joined Digital Arts, Inc., where he contributed to the development of security products. In 2019, he transitioned to SecureBrain Corporation, also in Japan, with a primary focus on research and development in the field of cybersecurity. Since 2022, he has been concurrently enrolled in the doctoral program at the Graduate School of Informatics at Tokyo University of Information Sciences in Japan. His research interests encompass cybersecurity and network quality control. He holds memberships in IEEE, IEICE, and IPSJ.

Masaki Hanada was born in Japan 1973, received the B.E. degree in resources engineering from Waseda University in 1996, the M.S. degree in information science from Japan Advanced Institute of Science and Technology (JAIST) in 1999, and the M.S. and D.S. degrees in global information and telecommunication studies from Waseda University in 2003 and 2007, respectively. He worked at Waseda University and Tokyo University of Science. After joining Tokyo University of Information Sciences as an Assistant Professor in 2011, he has been a Professor in the Department of Information Systems, Tokyo University of Information Sciences, since 2019. His research interests include network QoS control, network resource control and management, and network security. He is a member of the IEEE, IEICE and IPSJ.

Atsushi Waseda was born in Japan 1977, received the B.E. degree in communication engineering from the University of Electro-Communications in 2000. He received his M.S. and Ph.D. in information science from Japan Advanced Institute of Science and Technology (JAIST) in 2002, and 2007, respectively. He worked at the National Institute of Information and Communications Technology and KDDI research inc. After joining Tokyo University of Information Sciences as an Assistant Professor in 2019. His research interests include information security, quantum security and privacy protection. He is a member of the IEICE and IPSJ.

Moo Wan Kim was born in Korea 1951, received B.E., M.E. and Ph.D degree in electronic engineering from Osaka University, Osaka, Japan in 1974, 1977 and 1980, respectively. He joined Fujitsu Lab. in 1980 and had been engaged in research and development on multimedia communication systems, Intelligent Network, ATM switching system and operating system. In 1998 he joined Motorola Japan and had been engaged in research and development on CDMA2000 system. In 2000 he joined Lucent Japan and had been engaged in research and development on W-CDMA system, IMS and Parlay. In 2005 he joined Tokyo University of Information Sciences and had been engaged in research on Ubiquitous Network. In 2022 he joined TA Tech. as a lecture.