An Automated Vulnerability Assessment Approach for WebAPI that Considers Requests and Responses

Toru Taya*, Masaki Hanada**, Yoichi Murakami**, Atsushi Waseda**,

Yuki Ishida***, Takao Mimura***, KIM Moo Wan** and Eiji Nunohiro**

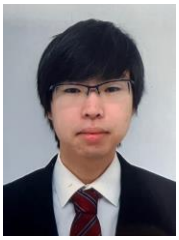
*Graduate School of Informatics, Tokyo University of Information Sciences, *4-1 Onaridai, Wakaba-ku, Chiba-shi, Chiba, Japan*

**Department of Informatics, Tokyo University of Information Sciences, 4-1 Onaridai, Wakaba-ku, Chiba-shi, Chiba, Japan*

****SecureBrain Corporation, Kioicho Bldg 7F, 3-12 Kioicho, Chiyoda-ku, Tokyo, Japan.*
g20004tt@edu.tuis.ac.jp, mhanada@rsch.tuis.ac.jp

***(Pt9)Abstract*— In recent years, WebAPIs are being published to allow external users to use Web services. On the other hand, the number of attacks that exploit WebAPI vulnerabilities is increasing. In order to prevent damage caused by abusing WebAPI vulnerabilities, the OWASP (Open Web Application Security Project) has published a guideline (OWASP API Security Top 10) describing the 10 vulnerabilities with the highest security risk in WebAPIs. However, the guideline does not describe the methods of attack and detailed countermeasures. Therefore, there are some vulnerabilities that are difficult to detect with existing WebAPI vulnerability assessment tools. In this paper, we propose a vulnerability assessment method that automatically obtains the WebAPI reference and repeatedly analyzes the requests through WebAPI and their responses. The proposed vulnerability assessment method will enable vulnerability assessment for vulnerability items that are difficult to be detected by existing vulnerability assessment tools among vulnerability items described in the guideline (OWASP API Security Top 10).**

***Keyword*— Vulnerability Assessment, WebAPI**



Toru Taya received Bachelor of Information Sciences from Tokyo University of Information Sciences, Japan, in 2020. Entered Graduate School of Informatics, Tokyo University of Information Sciences in the same year.

Masaki Hanada 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.

Yoichi Murakami received his Bachelor of Business Administration and Information Sciences from Tokyo University of Information Sciences, Japan, in 2000, his M.Sc. in Bioinformatics from the School of Life Sciences, University of Sussex, United Kingdom, in 2006, and his Ph.D. in Science from the Graduate School of Frontier Bioscience, Osaka University, Japan, in 2012. In 2017, he joined the Department of Informatics, Tokyo University of Information Sciences, as an assistant professor, and in 2019 he became an associate professor. His current research interests are in the areas of bioinformatics, machine learning, data mining and knowledge discovery.

Atsushi Waseda 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.

Yuki Ishida received the Bachelor's and Master's degree in Informatics from Tokyo University of Information Sciences, Japan, in 2014 and 2016, respectively. He joined SecureBrain Corporation in Tokyo in 2019, after participating in security product development at a software company. He is a software engineer and has been engaged in research and development for cyber security. He is a member of the IEICE and IPSJ.

Takao Mimura received the Bachelor of Business Administration and Information Science from Hokkaido Information University in Hokkaido, Japan in 2007. He joined SecureBrain Corporation in Tokyo, Japan in 2014 after participating in product development at software companies. He is a senior software engineer and has been engaged in research and development for cyber security.

Moo Wan Kim 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 has been engaged in research on Ubiquitous Network.

Eiji Nunohiro received the Doctor of Engineering from Nihon University. He worked at Hitachi, Ltd in 1985. After joining Tokyo University of Information Sciences as an Associate Professor in 2002, he has been a Professor in the Department of Information Systems, Tokyo University of Information Sciences, since 2007. His research interests include compiler and parallel algorithm in high performance computing, cyber security, programming training support system. He is a member of the IPSJ.