SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

レスポンスの情報を用いた WebAPIのアクセスコントロールに関する脆弱性診断方式

A Vulnerability Assessment Method for WebAPI Access Control Using Response Information

田谷 透 * 花田 真樹 † 村上 洋一 † 早稲田 篤志 † 石田 裕貴 ‡
Toru Taya Masaki Hanada Yoichi Murakami Atsushi Waseda Yuki Ishida
三村 隆夫 ‡ 布広 永示 †
Takao Mimura Eiji Nunohiro

キーワード WebAPI, 脆弱性診断

あらまし

近年，Web サービスの提供手法として，WebAPI が使用されるケースが増えている．その一方で，WebAPI の脆弱性を悪用した攻撃も報告されるようになっている．WebAPI に対する攻撃の被害を抑えるため，Web アプリケーションに関する取り組みを行う組織，Open Web Application Security Project（OWASP）は，セキュリティリスクの高い 10 の脆弱性項目について，報告書（OWASP API Security TOP 10[1]）を公開している．最も脅威とされる No.1 の脆弱性は，アクセスコントロールに関するものであり，ユーザに公開していない API の機能が使用されることによる意図しない情報が流出する脆弱性である．報告書には WebAPI に対する攻撃の具体的な手法や詳細な対策の手法が記述されていない問題点がある．また，WebAPI の脆弱性診断ツールにより脆弱性診断を行う際，ツールに対して膨大な数のパラメータの設定をユーザ自身が行う必要があり，設定情報の誤りや洩れが発生する可能性がある．上記の理由より，最も脅威なアクセスコントロールに関する脆弱性項目であっても，既存の脆弱性診断ツールによって検出が困難な場合がある．

そこで本研究では，WebAPI の最もセキュリティリスクの高い，アクセスコントロールに関する脆弱性に注目し，レスポンスの情報を使用した脆弱性診断手法を提案する．先行研究 [2] では，アクセスコントロールの脆弱性に属する No.5 の脆弱性に対するレスポンスを使用した脆弱性診断手法を提案し，評価を行った．Wordpress の WebAPI を使用した評価実験を実施し，既存脆弱性検出ツールでは検出が困難である記事改ざんの脆弱性の検出が可能であることを示した．本研究では，先行研究に続き，No.1 の脆弱性について，レスポンスの情報を使用した脆弱性診断手法を提案する．評価実験では，既存の脆弱性診断ツールで検出が困難である No.1 に該当する脆弱性診断を実施し，レスポンスを使用した脆弱性診断手法によって脆弱性の検出が可能であることを示す．

* 東京情報大学大学院 総合情報学研究科, 千葉県千葉市若葉区御成台 4-1, Graduate School of Informatics, Tokyo University of Information Sciences, 4-1 Onaridai, Wakaba-ku, Chiba-shi, Chiba, Japan.
† 東京情報大学 総合情報学部, 千葉県千葉市若葉区御成台 4-1, Department of Informatics, Tokyo University of Information Sciences, 4-1 Onaridai, Wakaba-ku, Chiba-shi, Chiba, Japan.
‡ 株式会社セキュアブレイン, 東京都千代田区紀尾井町 3 – 12 紀尾井町ビル 7F, SecureBrain Corporation, Kioicho Bldg 7F, 3-12 Kioicho, Chiyoda-ku, Tokyo, Japan.

参考文献

[1] OWASP, “OWASP API Security TOP 10 2019,” https://raw.githubusercontent.com/OWASP/API-Security/master/2019/en/dist/owasp-api-security-top-10.pdf, 2021/12/1.

[2] 田谷透，花田真樹，村上洋一，早稲田篤志，石田裕貴，三村隆夫，布広永示，“リクエストとそのレスポンスを考慮した WebAPI 脆弱性診断手法”，コンピュータセキュリティシンポジウム 2021 論文集，Vol2021，pp.1085-1092，Oct．2021．