Vol.2018-DPS-174 No.20
Vol.2018-CSEC-80 No.20
2018/3/6

Web アプリケーションの権限管理の不備を診断する手法の提案

反町孝平† 河内清人†

概要：インターネットに公開されている Web アプリケーションで利用する情報資産は，悪意のある攻撃者による攻撃から保護されなければならない．その中でも，権限によって利用できる機能が異なる Web アプリケーションは，権限管理が適切に行われていない場合，権限を越えた操作によって，システムや企業に損害を与える可能性がある．そのため，このような Web アプリケーションでは，権限によって適切に機能が制限されているかを，セキュリティ診断で確認する必　要がある．しかし，一般的なセキュリティ診断ツールでは，ページのリンクを遷移して診断を行うため，管理者専用ページなどの一般権限から遷移できないページに対して操作が可能かを診断できない．一方，手動の診断では，事前に権限毎に遷移情報を取得して，その情報の違いから，どの部分を変更してテストを実施すべきかを解析する専門性が必要であり，また，手動による確認のため，コストが掛かるという問題がある．本稿では，その解決策として，ツールで遷移できないページを自動で検出し，手動でリクエストを解析する必要のなく，人的コストの削減した診断を実現する方法を提案する．

キーワード：セキュリティ診断, Web アプリケーション, 権限管理

Proposal of testing method to insufficient authority management of Web application

KOHEI TAMMACHI† KIYOTO KAWAUCHI†

Abstract: Information assets used in web applications published on the Internet must be protected against attacks by malicious attackers. Among them, Web applications with different functions that can be used depending on authority may cause damage to systems and businesses by operations beyond authority, if authority management is not performed properly. Therefore, in such a Web application, it is necessary to confirm by security diagnosis whether the function is appropriately restricted by the authority. However, with a general security diagnostic tool, diagnosis is made by transitioning the page link, so it is not possible to diagnose whether operations can be performed on pages that cannot be transitioned from general authorities such as administrator exclusive pages. On the other hand, in the manual diagnosis, it is necessary to acquire the transition information for each authority in advance and expertise to analyze which part should be changed and the test should be carried out based on the difference in the information, There is a problem that cost is required for confirmation. In this paper, as a solution to that, we propose a method to automatically detect pages that cannot be transitioned with tools and realize diagnosis with reduced human cost without having to analyze requests manually.

Keywords: vulnerability testing, Web application, Authority management

1. はじめに

インターネットに公開されている Web アプリケーションが，企業のビジネスの上で重要な位置を占めるようになっている昨今，それらの脆弱性を悪用することによって，Web アプリケーションで使用されている機密情報の漏えいや，改ざん・停止などが発生するおそれがある．そのため，Web アプリケーションの脆弱性を悪用した攻撃は，組織や企業にとって，警戒しなければならない脅威である．

脆弱性を悪用した攻撃を防ぐためには，(1) Web アプリケーションをインターネット上に公開する前に Web アプリケーションに脆弱性が含まれていないかを確認する，(2) 公開した後には新たな脆弱性が発見されていないかを定期的に確認する，の二点が重要となる．

Web アプリケーションに存在する脆弱性を発見する方法として，セキュリティ診断が挙げられる．セキュリティ診断は，ツールまたは手動により対象の Web アプリケーションで使用されているソフトウェアのバージョン確認や，疑似的な攻撃を実施し，その応答によって脆弱性があるかを判断するものである．

一般的にセキュリティ診断で使用されているツールの診断の方法は，主に Web アプリケーション上のリンクを辿ることで画面遷移を行い，画面遷移で発生する HTTP リクエストの内容を，XSS（クロスサイトスクリプティング）や SQL インジェクション等の攻撃コードに変更し，そのレスポンスを正常の HTTP リクエスト時のレスポンスと比較することで脆弱性を判断する [1] [2] [3].

手動でのセキュリティ診断では，ツールではカバーできないような複雑な操作により画面遷移が起こる場合や，通信の詳細な解析を通して脆弱性を判定している．

セキュリティ診断の診断項目の一つに，Web アプリケー

* †1 三菱電機株式会社 情報技術総合研究所, Mitsubishi Electric Corporation, Information Technology R&D Center,

Vol.2018-DPS-174 No.20
Vol.2018-CSEC-80 No.20
2018/3/6

ションの権限管理の不備がある．これは，Web アプリケーションの操作権限がユーザの種別毎に適切に管理されているかを確認する項目である [4]．権限管理の不備に対する診断内容の例を次に示す．例えば，一般利用者の権限しか与えられていないユーザが，管理者用の機能にアクセスできるかの確認が挙げられる．

権限管理の不備の診断を考えた場合，ツールでは遷移可能な画面を基に診断を行う．特権のみが機能を提供するページへのリンクが一般権限で閲覧可能なページに現れていない場合，一般権限からそのようなページの存在をツールが感知することができず，権限管理の不備の脆弱性があったとしても，自動で診断することが難しい．診断する場合は，手動で一般権限と特権との画面遷移や HTTP リクエストの違いを比較し，特権にのみ存在する画面や機能を事前に洗い出し，強制的に一般権限で実行して利用できるかを確認することが必要となる．Web アプリケーションで発生する HTTP リクエスト毎に比較と実行を行わなければならないため，作業時間がかかる．そのため，セキュリティ診断に与えられた限られた時間の中で，開発する全ての Web アプリケーションで，権限管理の不備に対する十分な診断を実施することは，困難である．

そこで本稿では，権限管理の不備に対する診断について，診断実施者が，手動で，事前に HTTP リクエストの情報を把握することなく，人的コストを削減した診断方法を提案する．

本稿の構成を以下に示す．2 章で関連研究とその課題について述べる．3 章でその課題を解決するための提案方式を説明する．4 章で提案方式の有効性を考察し，5 章で本稿のまとめを行う．

2. 関連研究

権限によって異なるページが存在する Web アプリケーションの権限管理の脆弱性を検出する方法として，Michael BENDER らが提案した手法がある [5]．本手法は，Web アプリケーション URL に対して，特権ユーザによるアクセスが可能な URL リスト 1 と，非特権ユーザによるアクセスを行った場合の URL リスト 2 を比較し，URL リスト 1 にのみ存在する URL に，非特権ユーザがアクセス可能であった場合に脆弱性有りと判断する方法である．

本手法では，URL をキーにして，特権ユーザと非特権ユーザのアクセス可能なページの特定が可能となる．しかし，特権・非特権で同じ URL が存在し，その URL 内で権限によって使用できる機能が異なる場合は，検査の対象外となり，権限によって異なる機能に対する脆弱性は診断できないという課題がある．

Web アプリケーションの権限管理の不備に対してより詳細な診断をするためには，URL だけでなく，特権ユーザが送信するパラメータやその値に対して，非特権ユーザが利用可能かを確認する必要がある．

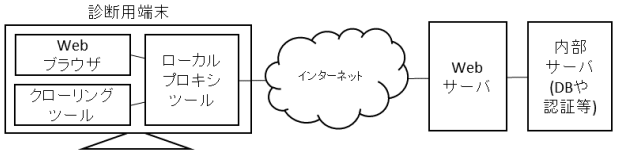

図 1　診断環境構成

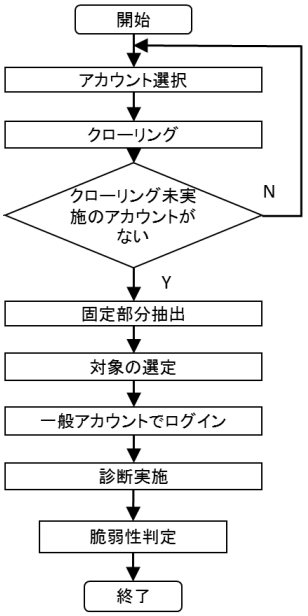

図 2　提案方式の全体処理フロー

3. 提案方式

本章では，権限管理の不備を正確に診断することができる診断方法を提案する．

3.1 診断環境の構成

本提案手法による診断環境は，一般的な Web アプリケーション診断ツールと同様，図 1 の構成をとる．

診断では，Web ブラウザやクローリングツールからの HTTP リクエストは，ローカルプロキシツールを通じて，Web サーバへ送信される．ローカルプロキシツールでは，HTTP リクエストとそのレスポンスをそれぞれ取得して，保存する．ここで保存されたデータを基に診断を進める．

3.2 提案方式の概要

提案方式では，権限によって遷移できる画面や使用できる機能が異なる Web アプリケーションに対して，権限管理の不備があるかを確認する．提案方式の概要を次に示す．

まず，各権限で発生する HTTP リクエストを取得する．特権アカウントで取得した HTTP リクエストの内容から，特権で固定されているパラメータや値を抽出し，一般権限のリクエスト内容と異なる部分を，一般権限アカウントのリクエストに挿入し，実行可能かを確認する．

また，診断の前提として，診断対象は，遷移できる画面や使用できる機能が権限によって異なる Web アプリケーションとする．異なる機能の具体例としては，Web ページ

Vol.2018-DPS-174 No.20
Vol.2018-CSEC-80 No.20
2018/3/6

内のリンクの有無，DB の登録・削除などの機能の使用権限，権限毎に割り当てられているパラメータ等が挙げられる．

3.3 提案方式の詳細

本節では，提案方式全体の処理を示し，各処理の詳細を説明する．提案方式の全体処理フローを図 2 に示す．

3.3.1 アカウント選択・クローリング

診断対象となる Web アプリケーション上で発生する HTTP リクエスト・レスポンスの情報を取得する．

提案方式では，特権によって送信される HTTP リクエストのうち，アカウントに関わらず固定な部分と，一般権限アカウント（以下，一般アカウント）で発生する HTTP リクエストの固定部分を比較するため，特権アカウント 2 つ以上，一般アカウント 1 つが必要となる．それぞれのアカウントが遷移可能なページの HTTP リクエストとレスポンスの内容を複数回（2 回以上）アクセスし，取得する．

アクセスにはクローリング等の技術を利用して，ページ内でアクセス可能なリンクを網羅的にアクセスする．アクセス時に発生した HTTP リクエストとレスポンスは，ローカルプロキシツールを通すことにより，全て取得することができる．

この時に取得したデータからは，表 1 に示すようなアカウントと URL の対応表である URL リストを作成する．作成した URL リストそれぞれに HTTP リクエストページ毎内にパラメータ名，パラメータの値，アクセスした権限などを，項目ごとに分割して保存したパラメータリストを作成する.する．パラメータリストの例を表 2 に示す.

3.3.2 固定部分抽出

同一の任意のアカウントで複数回取得したリクエストの内容から，①アクセスするタイミングによらず固定されているパラメータと値を抽出，②特権アカウントで取得した情報に対して，アカウントによらず固定されているパラメータを抽出する，という順番で処理を実施する．①と②の手法を次に示す.

①タイミングによらず固定となるパラメータ抽出

任意のアカウントで取得したリクエストの内容から，同じページに対して,1 回目と 2 回目(及びそれ以降)の HTTP リクエストとレスポンスが存在することとなる．同じページの HTTP リクエストの内容を比較すると，例えば，アクセス日時（Time）や Cookie のような，アクセスするタイミングによって値が変化するパラメータと，URL やアカウント名（userID），権限グループ（Auth）のような，アクセスするタイミングによらず値が固定となる固定パラメータに分類することができる（表 3）． これらの分類を，1 つのアカウントで発生する HTTP リクエスト全てに対して実施する．

1 つのアカウントに対するページ毎の比較が完了したら，比較を実施していないアカウントに対して同様の作業を実施し，取得した全ての HTTP リクエストに対して，変化するパラメータと固定パラメータを分類する．

表 1　権限毎の URL リスト例

ページID	権限	URL
特-1	特権A	http://xxx.com/Page1.html
特-2	特権A	http://xxx.com/Page2.html
特-3	特権A	http://xxx.com/Page3.html
・・・	・・・	・・・

表 2　URL 毎のパラメータリスト例

ID	ページID	パラメータ	値
特-1-1	特-1	URL	Page1.html
特-1-2	特-1	Time	xx:xx:xx
特-1-3	特-1	userID	Testuser1
・・・	・・・	・・・	・・・

表 3　同じページに対するリクエストの比較結果例

パラメータ名	1回目	2回目	判断※
URL	Page1.html	Page1.html	固定
Time	xx:xx:xx	yy:yy:yy	変化
userID	Testuser1	Testuser1	固定
Cookie	abcdefg	1234567	変化
Auth	2	2	固定

※固定：固定パラメータ　変化：変化するパラメータ

表 4　特権アカウントに対する固定パラメータの比較例

パラメータ名	特権アカウントA	特権アカウントB	判断※
URL	PageX.html	PageX.html	固定
userID	Admin1	Admin2	変化
Auth	1	1	固定

※固定：固定パラメータ　変化：変化するパラメータ

②アカウントによらず固定となるパラメータ抽出

次に，特権アカウントについては，1 つのページに対するそれぞれのアカウントで抽出された固定パラメータを比較し，アカウントによって変化するパラメータか固定パラメータかを分類する．この比較によって固定パラメータと分類されたパラメータは，アカウントによらず，全ての特権アカウントで同じ値として抽出することができる(表 4)．

3.3.3 対象の選定と診断の実施

Web アプリケーションに対して，特権アカウントと一般アカウントで得られた固定パラメータの情報から，権限管理の不備を確認する機能を選定し，診断を実施する．

本提案では，特権アカウントと一般アカウントの比較を，URL の差分，パラメータ名の差分，値の差分の 3 つのフローで実施し，それぞれのフロー内容に合わせた診断を実施する.対象の選定から診断までのフロー図を図 3 に示す.

①URL の差分がある対象への診断

はじめに，一般権限では，リンクが画面に表示されておらず，遷移ができない URL に対して，不正に遷移可能であるかを確認する．

特権アカウントと一般アカウントで遷移可能な URL を比較する．比較する URL は，権限毎に作成されている URL リストを対象とし，任意の特権アカウントと一般アカウン

Vol.2018-DPS-174 No.20
Vol.2018-CSEC-80 No.20
2018/3/6

トで同じ URL が存在するかを確認する.

この比較によって，特権アカウントにのみ存在する URL は，一般アカウントからは遷移できない URL であることが分かる．そのため，特権アカウントでのみ存在している URL を診断対象と判定する（表 5）.

診断対象となった URL に対して，一般アカウントからアクセスを行い，サーバからのレスポンスを確認する．アクセスするために URL 以外のパラメータが必要な場合は，固定パラメータのみを特権と同じものにして，Cookie などの変化するパラメータは，一般アカウント用に発行されたものを使用する.

診断と判断されなかった URL は，特権アカウントと一般アカウントが同じ画面にアクセスできることを示している.権限によらず同じ URL にアクセスできる場合であっても，リクエストの内容を改ざんすることによって，不正にアクセスできる可能性がある.HTTP リクエストの内容に差があるかを確認する手法を次項に示す.

②パラメータ名の差分がある対象への診断

①で対象と判断されなかった URL に対して，権限毎の HTTP リクエストのパラメータ名を比較し，一般アカウントの HTTP リクエストにパラメータ名を付加することによって，不正に機能が利用可能であるかを確認する.

権限毎に存在する同一 URL への HTTP リクエストに含まれるパラメータ名比較する．特権アカウントで使用しているパラメータ名が一般アカウントに存在している場合は，対象外として次のフローへ，存在していない場合は，そのパラメータ名が診断対象とする.

例えば，ユーザアカウントの設定について，特権アカウントで利用可能な機能がアカウントに対するパスワード設定（setPass），アカウント管理（Manage），アカウント削除（Delete）であったとする．これに対して，一般アカウントではパスワード設定のみが利用可能であり，その他の機能は利用できない，例えば，HTTP のリクエストにパラメータが存在しない場合，表 6 に示すようにパラメータの有無を分類することができる.

診断対象の URL において，一般アカウントで発生する HTTP リクエストに，対象となったパラメータ名を加えてサーバへ送信し，サーバからのレスポンスを確認する．その他のパラメータに関しては，一般アカウント用に発行されたものを使用する.

③パラメータの値の差分がある対象への診断

②で対象外となったパラメータ名の差分が無い画面に対して，パラメータの値を比較し，一般アカウントの HTTP リクエストのパラメータの値を特権アカウントのものにすることで，不正に機能が利用可能であるかを確認する.

権限毎に存在する同一 URL への HTTP リクエストに含まれる同一のパラメータの値を比較する.特権アカウントで使用しているパラメータの値が，一般アカウントと異なる場合は，その値を診断対象とする．異なっていない場合は，診断の対象外として，①のフローを別の URL に対して実施する.

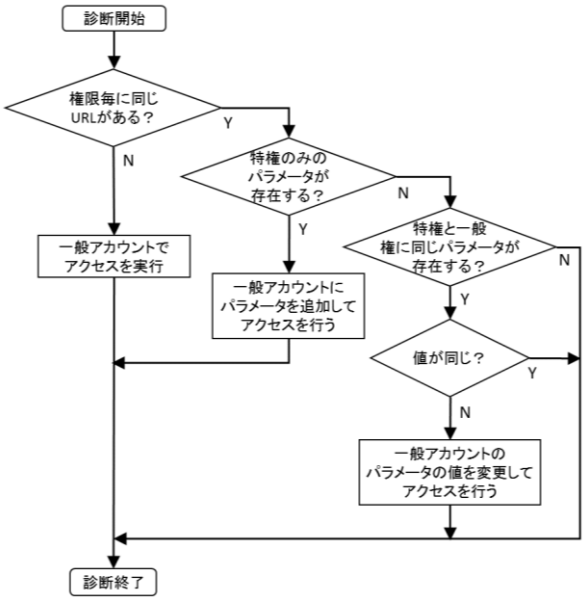

図 3　対象の選定から診断までのフロー図

表 5　権限毎の遷移可能 URL の比較

URL	特権アカウント※	一般アカウント※	判断
Page1.html	○	○	対象外
Page2.html	○	○	対象外
Page3.html	○	○	対象外
Page4.html	○	×	対象

※○：URLリストに対象のURLが存在する
×：URLリストに対象のURLリストが存在しない

表 6　権限毎のパラメータの有無の比較

パラメータ名	特権アカウント※	一般アカウント※	判断
setPass	○	○	対象外
Manage	○	×	対象
Delete	○	×	対象

※○：パラメータ名が存在する　×：パラメータ名が存在しない

表 7　権限毎の値の比較

パラメータ名	特権アカウント	一般アカウント	判断
Auth	1	2	対象

例えば，HTTP リクエストの Auth というパラメータの値が権限によって変化し，特権アカウントでは 1，一般アカウントでは 2 が設定されているような場合，Auth の値が診断対象となる（表 7）.

診断対象の URL において，一般アカウントで発生する HTTP リクエスト内で異なっているパラメータの値を，特権アカウントの値に変更してサーバに送信し，サーバからのレスポンスを確認する.

その他のパラメータに関しては，一般アカウント用に発行されたものを使用する.

3.3.4 脆弱性の判定

診断処理により得られたレスポンスを確認し，クローリ

ング時に取得した，サーバからのレスポンスを利用して脆弱であるかを判定する．

特権アカウントでアクセスした時に得られたレスポンスと，一般アカウントから改ざんした HTTP リクエストで得られたレスポンスが同じである場合は，サーバが権限に関係なく処理を進めていると判断できるため，Web アプリケーションの対象のページ・機能に権限管理の不備があるといえる．

特権アカウントと異なるレスポンスが得られた場合は，対象のページ（または機能）では，権限が異なる場合の処理を拒否しているとして，脆弱性はなしと判断することができる．

4. 考察

本稿で提案した，権限管理の不備に対する診断方法について考察する．

4.1 ツールでの診断について

一般的なツールでの診断を行う際，遷移可能な画面に対して，リクエスト中の変更可能なパラメータの値を，脆弱なパターンに書き換えて送信し，その応答によって脆弱性の有無を判断している．これは，1 つのアカウントが持つ権限内で，遷移可能なページ，または利用可能な範囲の機能に限られて診断されており，権限の範囲外の機能については，診断が行われない．

これまでの方法では，権限の不備を診断するためには，2 つ以上の異なる権限間で遷移可能な画面や機能を抽出して，それらの画面や機能が権限を越えて利用可能であるかを診断するという手動の操作が必要となるのが課題であった．

本提案方式で示した通り，アカウントを 2 種類以上使用して，それぞれの固定パラメータを取得して比較することにより，これまでツールのみでは実行できなかった権限の不備について診断を実施することができる．

4.2 作業時間について

権限管理の不備の診断を行うためには，診断実施者が手動によって，各権限で利用可能なページの機能を 1 つずつ比較して，どのパラメータをどの値に変更する必要があるがを確認するため時間がかかるという課題がある．

本提案方式では，権限毎のリクエストから，固定部分を抽出することで，比較すべきパラメータと値を予め決めることができる．そのため，手動で対象のリクエストを比較する必要がなく，作業時間を短縮させることが期待できる．

4.3 課題

本提案方式は，特権アカウントを 2 つ用いている．これは，複数の同一権限のアカウントを比較することで，ユーザ ID 等のアカウント固有のパラメータを除外するためである．アカウント固有を除外する理由としては，固有部分に脆弱性があった場合，同一権限内で他ユーザの操作が可能であるという脆弱性となり，これは，一般アカウントから特権アカウントの操作が可能かを確認するという本提案の目的とは異なるためである．

Web アプリケーションによっては，特権アカウントが 1 つしかない場合がある．この場合は，1 つの特権アカウントで複数回アクセスしたリクエストの固定パラメータができるが，アカウント毎の固有の値は抽出できないため，一般アカウントと比較した際に対象となるパラメータが増え，特権アカウントを 2 つ使用した場合より，作業時間が増えることが懸念される．

5. おわりに

権限によって，利用できる機能やページが異なる Web アプリケーションに対して，適切な権限の設定がされているかを診断する手法を提案した．従来研究では，一般権限を持つアカウントが特権のアカウントのみアクセス可能な URL へアクセスし，そのレスポンスが同じ場合はアラームを発生させるという手法であった．

本提案では，特権の 2 つのアカウントおよび一般権限のアカウントによる複数回のアクセスによって得られた情報から，権限固有のパラメータを取得し，そのパラメータの差分から，特権にのみアクセス可能なページや機能に対して一般権でアクセスが可能かを診断する手法を提案した．

6. 参考文献

1. **IBM.** IBM AppScan Source. (オンライン) https://www.ibm.com/jp-ja/marketplace/ibm-appscan-source.

2. **OWASP.** OWASP Zed Attack Proxy Project. (オンライン) https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project.

3. **PortSwigger Ltd.** Burp Suite Editions. (オンライン) https://portswigger.net/burp/.

4. **IPA.** 安全な ウェブサイトの 作り方 1.11 アクセス制御や認可制御の欠落. (オンライン) 2016 年 1 月 27 日. (引用日 : 2018 年 1 月 30 日.) https://www.ipa.go.jp/files/000017316.pdf.

5. **MichaelBENDER, ほか.** IDENTIFYING WEBPAGES ACCESSIBLE BY UNAUTHORIZED USERS VIA URL GUESSING OR NETWORK SNIFFING. 2017/0149782 A1 US, 2017 年.