高等教育機関での利用を想定した WebWolf 演習コンテンツの調査分析

牧 宣彰[1]　畑谷 成郎[1]　駒野 勝己[1]　渡辺 嶺[1]
盛 宸[1]　石川 大輔[1]　慎 祥揆[2]　瀬戸 洋一[1]

概要：サイバー攻撃の脅威が深刻化する一方，セキュリティ人材は不足状況にある．特に，予算に乏しい教育機関や中小企業においては，商用のサイバー演習システムの導入は困難である．従って，導入・運用コストの小さいオープンソースソフトウェアを活用してセキュリティ人材の育成を図る必要がある．また，サイバー攻撃は多様化かつ巧妙化しており，攻撃に対する適切な防御策の修得のためには，攻撃者の視点の理解が不可欠である．このため，従来行われてきた脆弱性診断を中心とする防御者の視点に立った演習のみならず，攻撃者を模した実践的な演習の実施は不可欠である．OWASP（Open Web Application Security Project）が公開している WebGoat および WebWolf は，オープンソースのセキュリティ演習ソフトウェアである．WebGoat が防御側の脆弱性診断演習であるのに対し，WebWolf は，攻撃側の演習環境の提供が試みられている．経済的かつ効果的なセキュリティ人材育成への活用が可能である．本稿では，WebWolf の機能と構成について調査を行い，高等教育機関のセキュリティ演習において WebWolf を用いることの有効性を分析した．

キーワード：サイバーセキュリティ教育，攻撃と防御，脅威，脆弱性，OSS

Survey of WebWolf Exercises Contents for Use in Higher Education Institutions

Nobuaki Maki[1]　Shigeo Hatatani[1]　Katsumi Komano[1]　Ryo Watanabe[1]
Chen Sheng[1]　Daisuke Ishikawa[1]　Sanggyu Shin[2]　Yoichi Seto[1]

Abstract: The threats of cyberattacks are expanding rapidly and the shortage of cyber security personnel is becoming a serious issue. However, it is difficult to utilize commercial cyber exercises system in educational institutions and small and medium sized enterprises because of limited financial capabilities. Therefore, open source exercise software without burden of the cost is highly beneficial for security human resources development. In addition, exercises to understand the attackers is needed to defend diversified and sophisticated cyberattacks. Thus, practical exercises carried out from the viewpoint of the attackers as well as the defenders are necessary. WebGoat and WebWolf released by OWASP are open source security exercises software. WebGoat provides vulnerability scanning exercises and WebWolf provides attackers side environment. In this paper, we investigated the function and configuration of WebWolf, and inspected whether WebWolf is effective in security exercises of higher education institutions.

Keywords: Cybersecurity Exercise, Cyberattack and Defense, Threat, Vulnerability, OSS

1. はじめに

近年サイバー攻撃は多様化・巧妙化しており，国内外で業務・サービス障害，情報漏えい，金銭被害が発生し，社会経済の発展や生活の安全・安心が脅かされている．2016 年 12 月には，ウクライナで，変電所がサイバー攻撃を受けて停電が発生し，2017 年 5 月には，英国の多数の病院で医療サービスが中断する被害が生じた．我が国でも，2015 年 5 月には日本年金機構が保有する個人情報約 125 万件の流出事案が発生し，2018 年 1 月には暗号資産（仮想通貨）の窃取事案が発生した．多大な経済的・社会的な損失が生じ得る状況にあり，サイバーセキュリティに対する社会の関心やニーズが高まっている[1].

我が国のサイバーセキュリティに関する施策の目標と実施方針を示すサイバーセキュリティ戦略では，セキュリティ人材の育成を課題として揚げている[2][3].

セキュリティ人材育成の取り組みとして，一部の大学や企業などではサイバーセキュリティの知識・技術を修得するため，専用のアプリケーションを用いたサイバー攻撃と防御を体験するサイバーレンジによる演習が実施されている[4][5].

商用のサイバーレンジによる演習では，仮想環境に構築したネットワーク上で，サイバー攻撃を想定した防御技術を体験学習できる．実際のマルウェアを用いるなど，現実

1 産業技術大学院大学
Advanced Institute of Industrial Technology
2 東海大学
Tokai University

に起こりうるシナリオを利用して，役割に応じた組織的な対応方法を学ぶことができ，高い教育効果が期待できる[6][7].

しかし，大学などの高等教育機関では，演習システムの導入コストの高さや演習環境の維持管理を行う人員の不足から，セキュリティ人材を育成するための教育環境の整備は進んでいない.

一方で，無償のセキュリティ演習ソフトウェアとして，WebGoat が公開されている[8][9]．WebGoat は，攻撃と防御の双方を体験学習する機能が不足し，攻撃手法の教育として用いるには不十分であったが，2017 年に，WebGoat に攻撃演習環境を付加することを目的として，新たに WebWolf が公開された．これらの OSS（オープンソースソフトウェア）の演習ソフトウェアは，過大なコスト負担なく実践的なセキュリティ人材に育成に資することが期待できる．そこで，WebWolf の機能と構成について調査を行い，高等教育機関のセキュリティ演習において WebWolf を用いることの有効性を分析した.

本稿では，2 章で脆弱性診断演習ソフトウェア WebGoat および WebWolf 演習の概要と攻撃側演習環境の必要性を概説し，3 章で WebWolf の構成と機能，4 章で WebWolf 演習の事例を紹介する．5 章では，高等教育期間のセキュリティ演習に WebWolf を活用することの有効性について検討する.

2. WebGoat および Web の概要

WebGoat は，OSS の脆弱性診断学習プログラムである．演習問題を通じて，Web アプリケーションの脆弱性の概要，検出および対策方法などを学習することができる. OWASP (Open Web Application Security Project) WebGoat Project に参画するセキュリティ専門家により開発，メンテナンスが行われている [10][11].

OWASP は，Web アプリケーションのセキュリティに関する，普及啓発等を目的とする非営利の国際オープンコミュニティであり，OWASP WebGoat Project は，OWASP 内のプロジェクトの一つである. OWASP は，セキュリティに関連する多くの企業や組織，専門家から，Web アプリケーションの脆弱性に関する情報を幅広く収集，対応策を調査し公表している.

WebGoat の演習プログラムは，Docker コンテナと JAR ライブラリの 2 つの形式で公開されており，PC にインストールし容易に演習環境を構築することが可能である．WebGoat を用いることにより，OWASP が収集した最新の情報に基づいて専門家が選定した優先度の高いセキュリティ上の課題について，体系的に学習することができる.

2018 年以前の WebGoat は，防御側の視点からの静的な脆弱性診断演習が中心であり，攻撃手法を理解するための攻撃者の視点からの演習が必要であった．このため，2017 年 11 月の WebGoat バージョン 8 のリリースの際に，WebGoat から WebWolf が分離され，攻撃側の環境を模擬する別個のソフトウェアとして公開された．WebWolf は WebGoat と連携して演習環境を構成する.

表 1 に示すように，WebGoat は，12 の演習テーマ，70 の演習問題がある．演習者は演習問題に解答することで脆弱性防御に関する知識・スキルを身につけることができる.

表 1　WebGoat 演習の概要

演習テーマ	演習数
1．Introduction	2
2.General	6
3.Injection Flaws	18
4.Authentication Flaws	10
5.Cross-Site Scripting	8
6. Access Control Flaws	6
7. Insecure Communication	1
8. Insecure Deserialization	4
9. Request Forgeries	6
10. Vulnerable Components	2
11. Client side	5
12. Challenges	5

WebWolf は，表 1 に示す演習問題のうち，図 1 に示すように攻撃用ファイルの作成・アップロードや，攻撃者・防御者とは別の第三のインターネット上の環境の使用など，攻撃者と防御者の行動を明確に区別することが演習者の理解に資する一部の演習問題について用いられている.

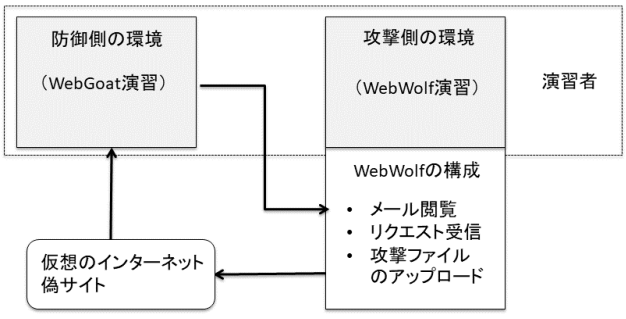

図 1　WebGoat と WebWolf の関係

3. WebWolf の構成と機能

3.1 WebWolf の構成

表 2 に示すように，WebWolf は，Home 画面のほか，WebGoat の演習問題を解答するための 3 つのサブシステムから構成される．

表 2　WebWolf の構成と機能の概要

構成	機能
1.Home	攻撃環境へのサインイン
2.Files	攻撃者による Web 上へのファイルアップロードを模擬
3.Mailbox	攻撃者のメールクライアントを模擬
4.Incoming requests	攻撃者が取得した HTTP リクエストの表示

3.1.1 Home

WebWolf 起動直後に表示される最初の画面であり，アカウントとパスワードを入力してサインインする．WebGoat と同一のアカウントを使用することにより，WebGoat と連動した演習を実施できる．

3.1.2 Files

攻撃者が作成した脆弱性を悪用する攻撃用ファイルを演習環境にアップロードする．実際の攻撃で，例えばクロスサイド・リクエストフォージェリのために攻撃者が悪意ある Web サーバに攻撃手段を仕込むことなどを模擬する．

3.1.3 Mailbox

攻撃者が使用するメールクライアントを模擬する．電子メールを利用したパスワードリセットに関する演習で用いる．

3.1.4 Incoming requests

攻撃者が取得した HTTP リクエストを表示する機能を有する．他のツールを用いて WebGoat からの HTTP リクエストの宛先を WebWolf に改変することにより，リクエストの内容を確認する．

3.2 演習問題

表 3 は，WebWolf を使用する WebGoat の演習問題である．

2019 年 1 月以降の WebGoat のリリース状況は次のとおりで，更改の頻度は高い．

- バージョン v8.0.0.M23（1 月 18 日更改）
- バージョン v8.0.0.M24（2 月 8 日更改）
- バージョン v8.0.0.M25（5 月 3 日更改）

WebGoat の演習問題数は，v8.0.0.M25 への更改の際に 48 問から 70 問に増加するなど，OWASP が収集している最新のサイバーセキュリティ上の課題に対応している．

表 3 は WebWolf を使用する演習問題を示す．問題数は，WobGoat の演習問題 70 問のうちの 9 問，機能の説明に関する演習問題を除くと 6 問となっており，現在も開発中である．

表 3　演習問題と機能

演習問題	Files	Mailbox	Incoming requests
1.Introduction Your own mailbox		○	
2.Introduction Landing page			○
3.Injection Flaws Blind XXE assignment	○		○
4.Authentication Flaws Email functionality with WebWolf		○	
5.Authentication Flaws Creating the password reset link			○
6.Requests Forgeries Basic Get CSRF Exercise	○		
7.Requests Forgeries Post a review on someone else's behalf	○		
8.Requests Forgeries CSRF and content-type	○		
9.Requests Forgeries Login CSRF Attack	○		

4. WebWolf 演習の事例

WebWolf を使用する演習問題の例として，クロスサイト・リクエストフォージェリを扱った Post a review on someone else's behalf を取り上げる．演習の流れ，演習を実施するにあたっての WebWolf の位置付け等は以下のとおりである．

4.1 概要

クロスサイト・リクエストフォージェリの脆弱性により，掲示板にユーザの意図に反した投稿を行わせる演習である．

クロスサイト・リクエストフォージェリは，図 2 に示すように，偽造したリクエストのサイトを跨いた送信を強要する攻撃手法である．例えば，攻撃者があらかじめインターネット上に攻撃用ファイルを配置し罠のリンクを設定，正規のウェブサイトにログインしたユーザを誘導し罠のリンクをクリックさせ，ブラウザにユーザの意図しないリクエストを送信させるなどする．

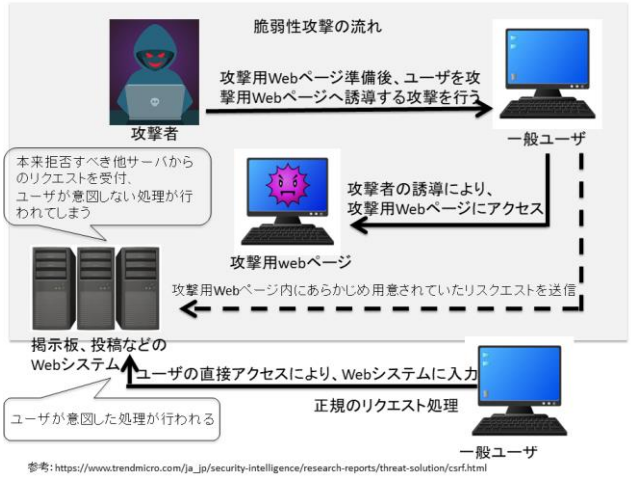

図 2　クロスサイト・リクエストフォージェリの概要

4.2 演習の構成

WebGoat は，正規の掲示板の Web サーバおよびユーザが書込みを行うブラウザの役割を担う．

WebWolf は，攻撃者が攻撃用ファイルをアップロードする悪意ある Web サーバの役割を担う．

WebGoat，WebWolf のほか，攻撃者は，現実の攻撃と同様に，OWASP ZAP などのペネトレーションツールおよびテキストエディタを用いて通信の傍受や攻撃ファイルの作成を行う．

4.3 演習シナリオ

図 3 は演習の流れを示す．WebGoat は，攻撃者がインターネット空間上に攻撃用ファイルをアップロードする際の悪意ある Web サーバの役割を担っている．攻撃者がファイルをアップロードする動作と，ユーザが誤ってリンクをクリックする動作を再現する際に使用される．

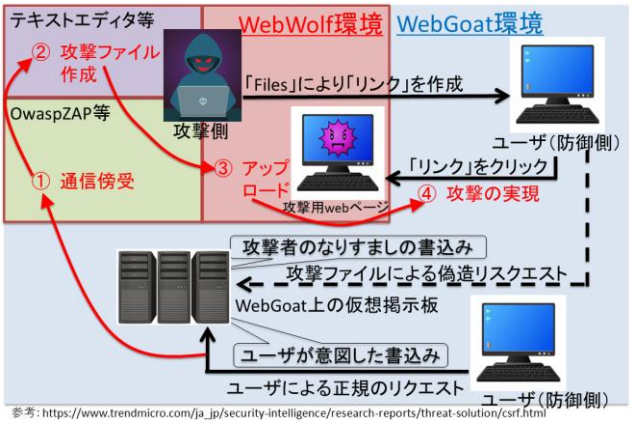

図 3　演習の流れ

① 通信傍受

WebGoat 上の掲示板のフォームに書き込みを行うのと同時に，ペネトレーションツールを使用し，ブラウザからのリクエストを確認する．当該演習の掲示板は，POST メソッドの HTTP リクエストメッセージボディにより，フォームに書き込んだ情報とユーザ固有の特定の値を引き渡す仕様になっている．

被害者による掲示板投稿の通信を攻撃者が傍受することを模擬している．

② 攻撃ファイル作成

テキストエディタを用いて，クロサイト・リクエストフォージェリ攻撃を行うための攻撃用 HTML ファイルを作成する．当該 HTML ファイルを読み込むと，①の投稿の際に使用されたユーザ固有の特定の値を窃用して偽の投稿を実行するよう，JAVA スクリプトを記載する．

攻撃者が，攻撃用ファイルを作成することを模擬している．

③ 攻撃ファイルアップロード

WebWolf の Files を使用し，②で作成した HTML ファイルを保存する．

攻撃者が悪意ある Web サーバに攻撃用 HTML ファイルをアップロードすることを模擬している．

④ 攻撃の実現

WebWolf の Files 画面に表示される「リンク」をクリックする．③で保存した HTML ファイルの JAVA スクリプトが実行され，攻撃者が用意した内容が投稿される．

ユーザの錯誤による罠リンクのクリックと，攻撃者のなりすましによるユーザの意図に反した掲示板書込みを模擬している．

5. セキュリティ演習における WebWolf の有効性検討

5.1 高等教育機関におけるセキュリティ演習

高等教育機関において，利用するセキュリティ演習プログラムは，導入・運営のコストが少ないことに加え，特に攻撃者の目線の理解を促すことに配慮し，十分な教育効果を発揮できることが求められる．具体的な以下の事項を満たす必要がある．

(1) 導入・運用コスト
導入・運用コストが高等教育機関における教育として実施するあたり過大でないこと

(2) 攻撃と防御の役割分担
攻撃側・防御側の手順が整然と区別され，演習者が混乱なく理解できること

(3) 攻撃者の環境・手法の理解
現実の攻撃者の環境や手法について学ぶことができること

(4) 演習環境の外部への影響
攻撃演習の影響が演習環境外部に及ぶことがないこと

WebWolf が要求事項を満たすか以下に検討した．

(1) 導入・運用コスト

WebWolf および WebGoat の演習プログラムは, Docker コンテナと JAR ライブラリの 2 つの形式で公開されており，PC にインストールし容易に演習環境を構築することが可能である. 商用のサイバー演習システムと比較して, 導入, 維持, 管理のためのコストや専門人員確保の負担は少ない．

(2) 攻撃と防御の役割分担

バージョン 7 以前の WebGoat では，攻撃側と防御側の行動の区別が不明確であり，受講者に混乱が生じる場合があった．その解決のため，バージョン 8 では，WebGoat とは別の演習ソフトウェアとして攻撃者の環境を模擬する WebGoat が導入された．これにより，攻撃側と防御側の行動を受講者が明確に区別しながら学習することが可能になり，受講者の理解に資することとなった．

(3) 攻撃者の環境・手法の理解

サイバー攻撃と防御対策を学習するためには，攻撃者が用いる環境や手法について理解することが不可欠である．WebWolf は，攻撃者が使用するツールや脆弱性の悪用方法について，演習を通じ学習しやすい構成となっている．また，現実の攻撃者が複数の環境を利用して攻撃を実施していることも体験することができる．

(4) 演習環境の外部への影響

演習を実施する際には誤って演習環境外に攻撃を行うことがないよう十分な注意が求められる．仮想環境上の WebWolf を用いることにより，攻撃は仮想環境の閉じたネットワークの内部に限られ，外部に影響を及ぼすことはない．インターネットから隔離された環境下で演習が完結するため，講習を実施する主催者および受講生は安全に学習が実施できる．

6. おわりに

近年のサイバー攻撃の増加に伴い，セキュリティ人材の不足は深刻な状況にある．しかし，高価なサイバーレンジ演習を実施可能な高等教育機関は限られ，セキュリティ人材育成は進んでいない．高等教育機関に受け入れやすく，教育効果の高いセキュリティ演習プログラムが求められている．

本稿では，オープンソースのセキュリティ演習プログラム WebWolf の機能，構成や演習シナリオを調査し，高等教育機関のセキュリティ教育で使用するにあたっての有効性について考察した．その結果，WebWolf 演習は，導入・運用のコストを要さずに攻撃側の演習環境が構築できることに加え，攻撃側と防御側の手順が明確に区別されるなど，コスト，教育効果の両面から，WebWolf の有用性が認められた．

現在, 開発中である WebWolf を利用する演習課題数は限られるが，今後演習コンテンツが拡充されれば，WebWolf による攻撃と防御を体験可能な演習環境を活用し，実践的なセキュリティ人材の効率的な育成することが期待できる．今後とも，OWASP WebGoat Project および WebWolf の開発の動向を注視し，新たな情報を入手次第，さらなる調査を行うこととしたい．

謝辞 本研究は JSPS 科研費 JP16K 19K03006 の助成と，東海大学総合研究機構「研究スタートアップ支援」の援助を受けて行ったものです．

参考文献

[1] 情報処理推進機構: 情報セキュリティ白書 2018, 2018 年 7 月.
[2] 内閣サイバーセキュリティセンター: サイバーセキュリティ戦略, 2015 年 9 月 https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf.
[3] 経済産業省: IT 人材の最新動向と将来推計に関する調査結果, 2016 年 6 月 http://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_report_summary.pdf.
[4] 情報通信研究機構: 平成 30 年度実践的サイバー防御演習「Cyder」の開催について https://www.nict.go.jp/press/2018/03/07-1.html.
[5] 中島滉介ほか: 「攻撃者目線」で学べるシステムセキュリティ実践的学習環境の提案, 日本ソフトウェア科学会第 30 回大会, 2013 年 9 月.
[6] 江連三香: サイバー攻撃に備えた実践的演習, 情報処理, Vol.55 No.7,2014 年 7 月.
[7] 株式会社ラック: 情報セキュリティの現状と動向について―サイバー演習の実施要領と演習事例―, 2015 年, 2 月

[8] 豊田真一,瀬戸洋一ほか: エコシステムで構成するサイバー攻撃と防御演習システム CyExec,
CSS2018，2018.10
[9] サイバーセキュリティ演習システム CyExec を用いた演習コンテンツの開発
SCIS2019, 2019.1
[10] OWASP WebGoat Project
https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
[11] Releases WebGoat/WebGoat
https://github.com/WebGoat/WebGoat/releases