Web アプリケーションに対する攻撃の動作を視覚化する教育支援システムの開発と評価

21G463　後藤祥仁（最所研究室）

XSS や SQL インジェクションを体験できるチャットアプリを対象とし，パケット転送を視覚することで攻撃手法のメカニズムを理解できる「Visual Website Attack」を開発した．評価した結果，教育効果があることが確認できた．

１．はじめに

XSS や SQL インジェクションなど，いまだにセキュリティリスクを持った Web アプリは多く，現在でも様々な被害事例がある[1]．このようなリスクを持ってしまう原因の一つとして，開発者にセキュリティに関する知識が不足している点が挙げられる．これに対する解決策として，セキュリティ演習がある[2]．セキュリティ演習は企業や大学で増えており，攻撃手法や対策方法などを学ぶことができる．これらの演習では，前提として必要な IT に関する知識や，実務経験のない大学学部生には難しい．

そこで，本研究ではそのような学生に理解を促す「Visual Website Attack(VWA)」を開発した．VWA の目標として，目標(1)：大人数が一斉に演習システムを利用できる，目標(2)：受講者がサーバやネットワーク内部の動きを理解できる，目標(3)：攻撃者視点で攻撃手法を理解できる，の 3 つがある．

２．要件定義

3 つの目標から要件として，要件(1)：Web アプリ上で動作するシミュレータとして再現する，要件(2)：チャットアプリ内部の動きを視覚的に再現する，要件(3)：受講者の入力によって視覚内容を変化させる，の 3 つを導く．要件(1)から目標(1)を達成するため，サーバへの負荷を下げるよう，受講者のブラウザ上で動作するシミュレータとして再現する．要件(2)から目標(2)を達成するため，チャットアプリでの動作をステップごとに矢印を用いて表現することで，チャットアプリ内部の動きを視覚的に再現する．要件(3)から目標(3)を達成するため，受講者が自身で調べた様々な手法をシミュレートし，それによって攻撃が成功，または失敗する体験ができるインタラクティブなシステムを実現する．

３．実装

VWA の UI を図 1 に示す．　Ⓐに被害を受けるチャット，Ⓑに受講者が攻撃者として入力するページ，Ⓒにチャットアプリの提供サーバと矢印で表示しているパケット，Ⓓにデータベーステーブルがある．

要件(1)実現のため，先ほど説明した UI とそれを動作させるためのシミュレータ機能を JavaScript で開発した．シミュレータ機能には，防御処理機能，ログイン処理機能，データベース処理機能，パケット転送表示機能がある．これらの機能が動くことにより，シミュレータ特有のステップ実行が可能となる．

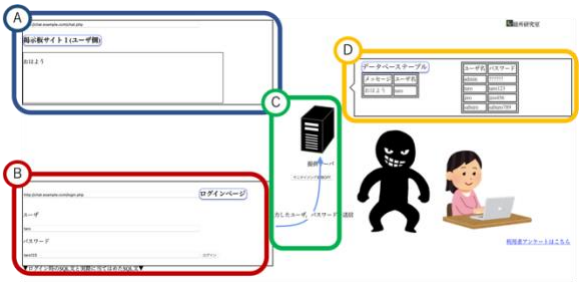

図 1 VWA の UI

要件(2)実現のため，パケット転送表示機能を開発した．これは，パケットを矢印として表示するために必要な機能である．図 1 のⒸにあるように，パケット転送の目的とともに表示される．矢印はボタンをクリックするごとに順次表示され，図 1 の場合，次は提供サーバからデータベーステーブルに矢印が遷移される．

要件(3)実現のため，データベース処理機能，チャット処理機能，ログイン処理機能，防御処理機能を開発した．データベース処理機能は，Ⓓのように再現し，処理ごとにデータの参照または追加を行う．チャット処理機能では，Ⓐのように再現し，チャットとしての動作を行う．XSS を行えるよう，html タグを容認している．ログイン処理機能では，ログイン動作を行う．SQL インジェクションを用いた不正ログインを行える．防御処理機能では，サニタイジング処理を行う．Ⓒの提供サーバ下にボタンがあり，それをクリックすることで，サニタイジング処理が可能になる．

４．講義想定

まず，VWA で扱う XSS，SQL インジェクションの用語説明を行う．次に，VWA の説明と操作方法を，攻撃例を提示しつつ示す．その後，受講者が操作する．受講者は，データベーステーブルに登録されているユーザとパスワードを使ったログインや，チャットでのメッセージ送信を行う．その後，不正ログインや XSS を試すことで，攻撃手法を理解する．最後に，防御処理を行い，今までできた攻撃ができなくなったことを確認する．

５．評価実験

設定した目標が達成できているかを確認するための評価実験を行う．評価実験対象者は，セキュリティ演習を受ける前提として必要な IT に関する知識が乏しく，実務経験のない理系大学生 81 人であ

る．対象となる受講者を，座学と VWA を使うグループ A，座学のみを行うグループ B に分けて，それぞれの結果を比較する．いずれも同じ演習時間となっており，グループ A の座学では各種攻撃の用語説明，グループ B の座学では，用語説明や図解，事例，防御手法の紹介をしている．評価は 2 日(2022/12/21，2023/1/11)に渡って行う．評価方法として，4 択問題からなるテスト，アンケート形式の 5 段階評価，システム操作のログを用いた評価である．テストは演習前，演習後，数週間後の 3 回実施し，XSS を 2 問，SQL インジェクションを 2 問，SQL インジェクションによる不正ログインを 1 問実施する．アンケートでは，両グループ共通質問やグループ A のみに聞く質問，2 日目に聞く質問がある．操作ログは，VWA を利用した受講者のログを収集し，どんな操作をしたかを見て評価する．

５．結果と考察

設定した目標を達成できているかを述べる．目標(1)について，39 人同時に演習を行ったが，特にトラブルなく，ログ上で通信エラーを示す内容もなかった．また，グループ A に聞いた VWA の操作方法に関するアンケートの 5 段階評価において，上位 2 つを回答した割合が 71%であったこと，またアンケートの自由記述においても特に言及されなかったことから，目標(1)が達成できたと考えられる．

目標(2)について，自由記述で，「どういう処理を行なっているか分かりやすかった」「流れが分かりやすい」といった，データの流れがわかりやすい評価を得られた．したがって，目標(2)が達成された．

目標(3)について，図 2 の平均点の推移より，グループ A の演習後の点数が上がっていることがわかる．また，アンケートでの 5 段階評価において，XSS と SQL インジェクションの理解度を図る設問で，6 割以上の受講者が，上位 2 つを回答している．したがって，目標(3)が達成されている．

しかし，図 2 を見てわかる通り，グループ B の方が事後テスト 1 の点数が高い．これについては，座学で行った内容が原因と考えられる．座学では，4 択問題の答えに直結するような説明を行った．反対に，グループ A ではそのような説明をしていない．その直後で事後テスト 1 を実施したため，グループ B は大きく点が上昇した．

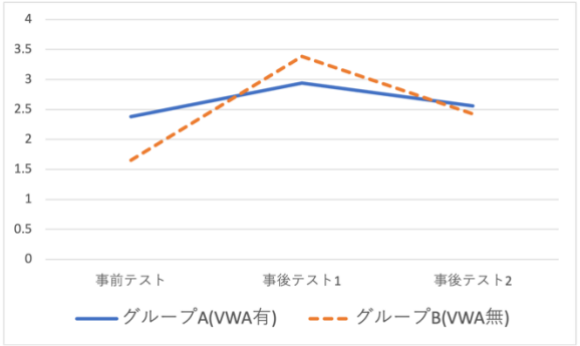

図 2 各グループの平均点の推移

表 1 不正ログインに関する問題の正答率

	事前テスト	事後テスト 1	事後テスト 2
グループ A	13%	35%	35%
グループ B	12%	38%	19%

また，事前テストと事後テスト 2 を比べた場合，グループ B の方が，点数が上昇していた．そこで，問題の種類ごとにグループごとの点数の比較を行う．その結果，不正ログインに関する問題について，グループ A とグループ B で顕著な差が出た．各グループの各テストの正答率を表 1 に示す．事前テスト，事後テスト 1 の正答率はほぼ同じであった．しかし，事後テスト 2 ではグループ A が 35%と前回と同じ正答率だったのに対し，グループ B では 19%となった．そのため，攻撃手法の理解については効果があることがわかる．

グループ A について，より詳細にみる．操作ログから，一定量の操作をした受講者(インタラクティブが高い)とそうでない受講者(インタラクティブが低い)の 2 つに分けた．高い受講者の各テストの点数分布を図 3，低い受講者の各テストの点数分布を図 4 に示した．その結果，インタラクティブが高いものは，事後テスト 1 で大幅に点数上がっており，反対にインタラクティブが低いものは，点数が上がっていない．したがって，インタラクティブ性が高いことは，受講者に対して有効であることがわかる．

文献

1) IPA“ソフトウェア等の脆弱性関連情報に関する届出状況[2022 年第 3 四半期(7～9 月)]”, https://www.ipa.go.jp/files/000103389.pdf(参照 2023.1.19)
2) 八代 哲，田邉 一寿，齋藤 祐太，齋藤 孝道，“体験型サイバーセキュリティ学習システムの提案と再評価”，マルチメディア，分散，協調とモバイル (DICOMO2018) シンポジウム pp.1809-1816，2018

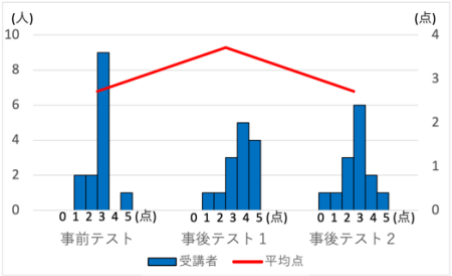

図 3 インタラクティブ性が高い受講者の点数分布

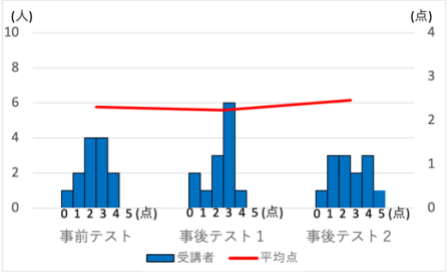

図 4 インタラクティブ性が低い受講者の点数分布