初学者を対象としたクロスサイトスクリプティングの学習支援に関する研究

A Study on Learning Support for Cross-site Scripting for Beginning Students

永井 弘輝[*1], 松本 慎平 [1]
Koki NAGAI[*1], Shimpei MATSUMOTO[*2]
[*1] 広島工業大学情報学部
[*1] Faculty of Applied Information Science, Hiroshima Institute of Technology
Email: {bl19067, s.matsumoto.gk}@cc.it-hiroshima.ac.jp

あらまし：Web アプリケーションにはセキュリティ機構が備わっているため，セキュリティに関する知識がなくても堅牢なアプリケーションが作れる．しかし，開発過程でセキュリティ機構が無効化される場合があることからセキュリティや脆弱性の知識が必要である．その一方で，セキュリティは応用的な内容であり，学習に負荷がかかる。そこで、本研究では初学者に対してクロスサイトスクリプティングの脆弱性について Web アプリケーション上で学習できるシステムを開発し，脆弱なコードを修正する過程の有用性を検証した．
キーワード：Web セキュリティ，クロスサイトスクリプティング，セキュアコーディング

1. 緒言

Web アプリケーション開発現場ではフレームワークを用いることが主流である．このようなフレームワークは基本的なセキュリティ機構が標準で備わっているため，開発者はセキュリティを意識せずとも堅牢なアプリケーションを作れるようになった．しかし，フレームワークやライブラリによって全ての脆弱性が保護されるわけではなく，これらを適切に使用しなければ脆弱性を作り込んでしまう．Web アプリケーションに対する攻撃を学習するためには，座学による学習だけでなく，実践型のセキュリティ演習が必要だとされている．ただし，脆弱性の学習は応用的な内容であり，セキュリティに関する学習は，情報工学や計算機工学などの前提知識を持つ者などが学習する発展的な要素であると考えられる．そのため，初学者が脆弱性について学習するのは容易ではないと考えられる．その一方で，独立行政法人情報処理推進機構(以降，IPA)の報告[(1)]から脆弱性の実践的教育に関する社会からの要求は高いということが分かる．従って，セキュリティの学習は社会から強く求められているということから，初学者にとって学びやすく，かつ効果的な脆弱性の演習環境が必要だと言える．本研究では，初学者を対象とし，Web アプリケーションに対するクロスサイトスクリプティング(以降，XSS)の学習支援を目的として，実践的な学習システムを提案する．XSS の学習に対して，コーディングを行いながら経験的に知識を習得することの有用性を明らかにする．なお，本研究では，IPA が主催する技術者試験のレベル 3 付近の学習者を初学者と位置付ける．

2. 脆弱性学習の必要性

XSS は Web アプリケーションの脆弱性を悪用した攻撃のひとつである．図 1 に XSS を利用した攻撃シナリオの一例を提示する．

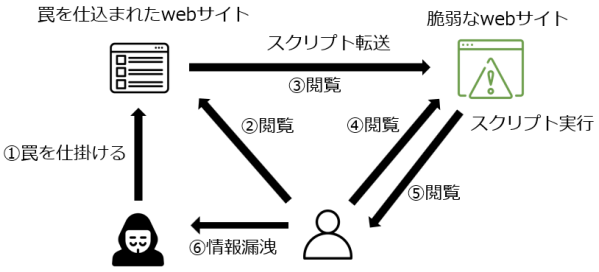

図 1　XSS の攻撃シナリオ

IPA が 2022 年第 1 四半期に公開したソフトウェア等の脆弱性関連情報に関する届出状況では，ソフトウェア製品の脆弱性の原因別の届出状況に関して，Web アプリケーションの脆弱性が全体の 55%と半分以上を占めていた．そして，届出された脆弱性がもたらす影響別のうち，XSS の被害が最も多い割合を占めていた．XSS の学習において格納型と継続型と DOM 型の概念理解とコーディングの観点から対策する必要があり，Web アプリケーション開発を行う初学者に対して更なる教育が必要だと言える．

3. 関連研究

セキュアな Web アプリケーションを開発できる技能を養成することを目的とした学術的な取り組みがいくつか行われている．

竹下らは，WebGoat という攻撃方法理解用のツールと組み合わせたウェブサイト製作者向け脆弱性対策 e ラーニングシステム VulCES を開発した[(2)]．また．岸本らは，仮想環境上で脆弱な Web サーバを用意して攻撃演習をする上で必要な脆弱性の発見方法の学習を重点的に支援できるようしたシステムを開発した[(3)]．仮想環境上で演習用の Web サーバを構築し、ローカルプロキシツールを用いて，XSS の脆弱性を探し，ペンテストツールを用いて攻撃を行った．

実験ではシステムを利用した学習と座学のみで学習したグループを用意してそれぞれの学習の前後にXSS に関する事前・事後テストを実施し，2 グループの事前・事後テストの結果，システムを利用した学習が座学で学習したグループよりも点数が上昇した．以上の結果から，システムが XSS 対策の学習を支援できたと結論付けた．しかし，先行研究では，ペンテストツールを多く利用していることから，Web アプリケーションセキュリティの前提知識が少ない初学者において XSS の学習が困難であると言える．さらに，比較対象がシステム上で学習したグループと座学のみで学習したグループで分けられており，ハンズオン学習の後に脆弱なソースコードを修正することの必要性は明らかになっていない．

4. 学習システム

セキュアコーディングの学習における重要性を評価するために，CureVuln[4]を参考にしたシステムを作成した．今回はこのシステムを参考にして，XSS に重点を置いた学習を行った．システムの詳細についてホスト OS は Windows10, 使用言語が Python3.7, Web フレームワークには Bottle と Flask を使用した．また，ミドルウェアには Docker と SQLite3 などを利用した．Web ブラウザ上で XSS を利用した脆弱性によって不正なスクリプトを実行させ，その後，XSS の解説を読み進めながら最後にエディタ上で脆弱なソースコードを修正してもらう．最後に Web フォームに不正なスクリプトを実行しても対策がされていることを確認する．システムの構成図及び学習画面の一例を図 2 に提示する．

図 2　格納型 XSS の学習画面

コーディングを行わない学習では，Damn Vulnerable Web App(以降, DVWA)を使用する．DVWA は意図的に脆弱性が含まれており，OS が Ubuntu10.05, Web サーバ側は Apache2.0, MySQL5.0.5, 言語は PHP5.3.1 で構成されている．DVWA を利用した学習では，まず Web 上で XSS を体験し，次に解説を受けた後，XSS の対策が施されている Web フォームで実行し，対策されていることを確認する．

5. 実験

本研究の被験者は基本的なコンピュータ操作に習熟しており，プログラミングの基本を理解している情報学を学習中の大学 2 年生～大学院生 1 年生 20 名である．最初にプレテストを用意して，最大 15 分間実施した．その後，平均・分散が均一になるよう実験群・統制群に群分けてプレテストから十分な時間を空けた後，実験群では，CureVuln を参考にして作成したシステムを利用して学習し，統制群では，DVWA を利用して学習をした．学習を終えた後，ポストテストを用意して最大 15 分間で実施した．そして最後に，認知負荷理論とフロー理論に関するアンケートへ回答した．実験結果について，実験群及び統制群のポストテストの結果を図 3 に提示する．

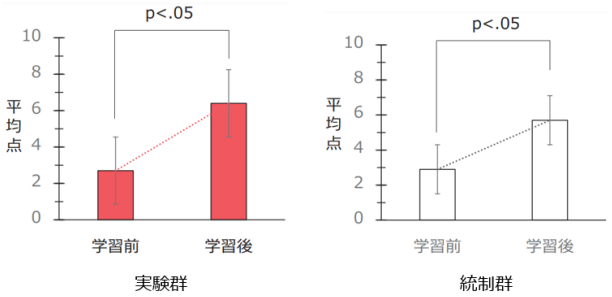

図 3 実験群と統制群のテスト結果

Welch の t 検定(両側)の結果，2 群の間に有意な差は示されなかった．一方，実験群の平均点は統制群よりも高かったため，提案システムは従来の学習方よりも効果的な可能性が示されたと言える．そして，テストにおける Welch の t 検定(両側)の結果，どちらも成績が有意(p<.05)に向上していることから，学習方法自体の適切性を確認できた．

6. 結言

本研究では，初学者に対しても応用的な内容である XSS の学習支援をすることを目的して行った．その結果，提案システムを用いた学習は一般的な学習よりも効果的な可能性があるということが示された．

参考文献

(1) 情報処理推進機構：“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 1 四半期(1 月~3 月”https://www.ipa.go.jp/files/000097930.pdf
(2) 竹下数明，小林偉昭:“脆弱性対策教育のための e ラーニングシステムの開発と評価”，コンピュータセキュリティシンポジウム 2009 (CSS2009) 論文集, 2006, 第 8 号, pp.1-6 （2009）
(3) 岸本和理，井口和信:“仮想マシンを活用したクロスサイトスクリプティングの実践的演習システム”，第 82 回全国大会講演論文集, Vol.1, pp.505-506 （2020）
(4) 森田浩平,松本慎平:“セキュアコーディング学習支援システムの開発”,2017 年度教育システム情報学会学生研究発表会講演論文集, pp.189-190 （2018）