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

竹下 数明† 小林 偉昭§ 佐々木 良一‡
†‡東京電機大学 §独立行政法人情報処理推進機構
†‡101-8457 東京都千代田区神田錦町 2-2
†takeshita@isl.im.dendai.ac.jp §hd-koba@ipa.go.jp ‡sasaki@im.dendai.ac.jp

あらまし ウェブに対する SQL インジェクションやクロスサイト・スクリプティングなどの脆弱性を悪用した攻撃が増加している．著者らは先にこれらの攻撃に対するセキュリティ意識の向上のための教育コンテンツを開発してきた．しかし，適切な対応のためには意識付けだけではなく，不正の仕組みや防止策も学習する必要がある．適切な防止策を理解するためには攻撃方法の理解が不可欠であると考え米国で開発された 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とコンテンツを開発した．本稿では，それらの概要と評価について報告する．

キーワード セキュリティ教育，脆弱性，E-learning，WebGoat

Development and evaluation of an e-learning system for vulnerability countermeasures education

Kazuaki Takeshita† Hideaki Kobayashi§ Ryoichi Sasaki‡
†‡Tokyo Denki University §INFORMATION-TECHNOLOGY PROMOTION AGENTY, JAPAN
†‡2-2 Kanda Nishiki-Cho Chiyoda-Ku Tokyo, 101-8457 Japan
†takeshita@isl.im.dendai.ac.jp §hd-koba@ipa.go.jp ‡sasaki@im.dendai.ac.jp

Abstract The number of attacks that abused weakness such as SQL injection or cross site scripting to WEB site is increasing rapidly. In first, we developed education contents for improvement of the security awareness for these attacks. However, it is necessary to learn not only the consciousness charge account but also structure and the preventive measures against injustice for the appropriate correspondence. We thought that the understanding of the attack method was indispensable to understand appropriate preventive measures. For this reason, we developed a vulnerability countermeasures e-learning system and content that was put together with a tool called "WebGoat" developed in U.S.A that teaches attack method. This paper describes about summary and evaluation of those contents.

Key Word Security education, Vulnerability, E-learning, WebGoat

1. はじめに

近年，ウェブに対する SQL インジェクションやクロスサイト・スクリプティング（以後 XSS と称す）などの脆弱性を悪用した攻撃が増加している．独立行政法人情報処理推進機構（以後 IPA と称す）の“ソフトウェア等の脆弱性関連情報に関する届出状況”[1]によると，IPA に報告された脆弱性届出件数は 2007 年に約 1700 件であったが，2009 年には約 5660 件にまで増加している．また，そのうちウェブサイトに関する届出が全体の 83%を占めている．そのため，各ウェブサイト製作者はウェブに対する脆弱性の確認と対策の実施を行う必要があるが，脆弱性の修正状況は非常に低く，具体的な脆弱性の対策を知っている人も少ない．そこで著者らは先にウェブの利

用者やコンテンツ作成者など一般向けに「いかに脆弱性を悪用した攻撃が甚大であるかを認知させ，セキュリティ意識の向上を目指す」ことを目的とするサウンドノベル形式のゲームによる教育コンテンツ「安全なウェブサイト運営入門」[2]を開発した．しかし，適切な対応のためには意識付けだけではなく，不正の仕組みや防止策も学習する必要がある．適切な防止策を理解するためには攻撃方法の理解が不可欠であると考え米国で開発された 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．本稿では，それらの概要と評価について報告する．

2. VulCES の概要

VulCES （**Vul**nerability **C**ountermeasures **E**-learning **S**ystem）とは 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教育システムであり, Windows 上で動作する WBT（ウェブベーストレーニング）形式のシステムである（図 1 参照）．脆弱性の意識付けだけでなく，不正の仕組みや防止策を啓発する．また安田らが開発した DMD（Digital Movie Director）[3]で作成したアニメーションも使用できるようになっている．VulCES の全体を制御するためのプログラムを VulCES-Basic と呼び，それは HTML で書かれている．

ユーザはブラウザをもって VulCES-Basic の出力を表示し，脆弱性の教育コンテンツを選択し，学習する．教育コンテンツについては 3.5 節で紹介するが，ユーザはある決められた順番でしか学習できないように設定した．ただ，一度学習したコンテンツはいつでも復習できる．また, 攻撃方法を学ぶ際 WebGoat の機能を利用し脆弱性の疑似攻撃を行ったときの結果を表示するようにした．

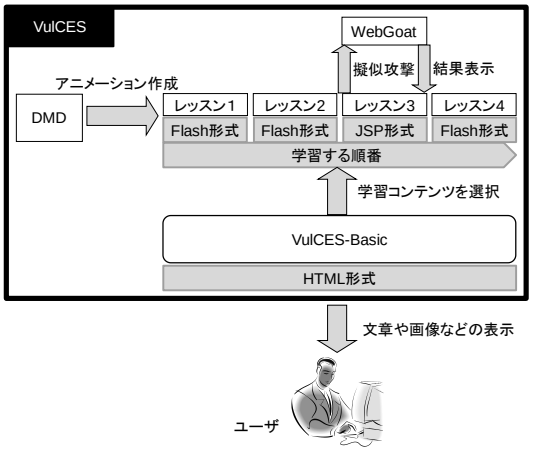

図 1　VulCES システムの構成

3. XSS 対策教育用の VulCES

今回, 著者らは XSS 脆弱性対策教育を行うため VulCES を用いてコンテンツを作成し，評価を行った．VulCES を用いた XSS 脆弱性対策教育用に作成したコンテンツを VulCES-XSS と称す.

3.1. VulCES-XSS の概要

VulCES-XSS は，XSS 脆弱性の概要，攻撃方法, 対策など総合的な XSS 教育を効果的に行うことを目的としている．VulCES-XSS では学習効果を高めるために以下の特徴を持たせている.

- 行動することによって学ぶシナリオ型教育を採用する
- DMD によって作成した対話形式のアニメーションを使用する
- WebGoat の機能を利用する
- シナリオの後に確認テストを実施する

3.2. シナリオ型教育

著者らは行動することによって学ぶシナリオ型教育システムを採用し，ユーザの動機づけを行い，効果的に達成できるように設計した．そのため，VulCES-XSS の構成要素として学習目標，使命，役割などを設定した．作成した VulCES-XSS の構成要素を表 1 に示す.

表 1　VulCES-XSS の構成要素

構成要素	作成したeラーニング
学習目標	XSS脆弱性の攻撃手法や対策を身につける
使命	ウェブサイトを脆弱性がないように設計できること
役割	ウェブサイト製作及び運営者（部下）
ストーリー	XSS脆弱性について講習を受けること

3.3. DMD の使用

DMD とは，主語，述語，目的語等をリストから選択するだけで，容易にかつ短時間で 3 次元 CG アニメーションを作成できるソフトである．さらに、自分の好みでカメラワークを工夫したり、BGM や効果音をつけることで、より本格的な演出をつけることも可能である．

多くの e ラーニングは「モチベーションの維持が困難」,「コンテンツがつまらない」などの問題が指摘されており[4]，それらの問題を解消するためには，ストーリーの一部としてアニメーションを用いることで e ラーニングの魅力が増すとされている．

VulCES-XSS におけるキャラクター同士の会話部分のアニメーションを DMD で作成して使用した（図 2 参照）．DMD では登場人物は全部で 48 人用意されており、その中から 2 人選択し使用した．

図 2　DMD で作成したアニメーション

3.4. WebGoat の使用

WebGoat とは非営利組織 OWASP が提供する体験型セキュリティ教育システムであり，わざと脆弱に作られた J2EE ウェブアプリケーションとそのウェブアプリケーションを使って脆弱性を学ぶための問題集で構成されている（図 3 参照）[5]．問題に沿って脆弱なウェブアプリケーションを擬似攻撃することで，ウェブアプリケーションの脆弱性を学ぶことを目的としている．

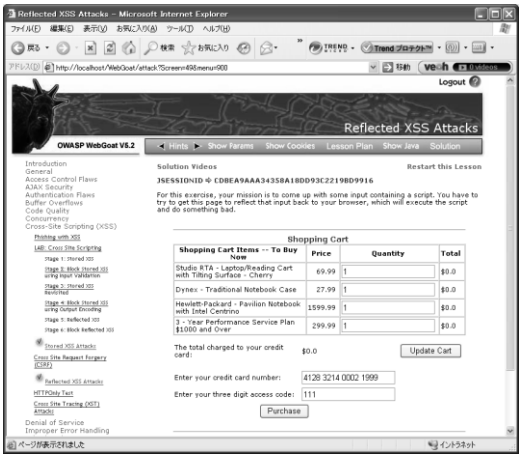

図 3　WebGoat の画面

VulCES-XSS では，WebGoat の機能を利用し，XSS 脆弱性の擬似攻撃を行った際の影響を確認できるようにした．

また，WebGoat に対する攻撃において WebScarab[6]を用い，HTTP リクエストやレスポンスの内容を確認するようにした．WebScarab とは同じく非営利組織 OWASP が提供するプロキシツールであり，HTTP リクエストやレスポンス内容を書き換えることができる．WebGoat のレッスンの中には HTTP リクエストの書き換えが必要なレッスンがある．そのため，図 4 のようにブラウザと WebGoat の間に WebScarab を挟み，WebScarab 経由で HTTP リクエストやレスポンスの通信を行うように変更する．

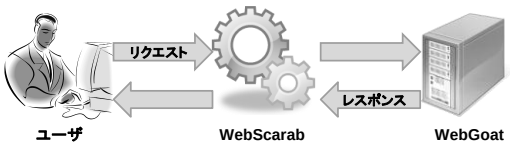

図 4　WebScarab の概要

3.5. コンテンツの流れ

VulCES-XSS のコンテンツを導く全体の流れを図 5 に示す.

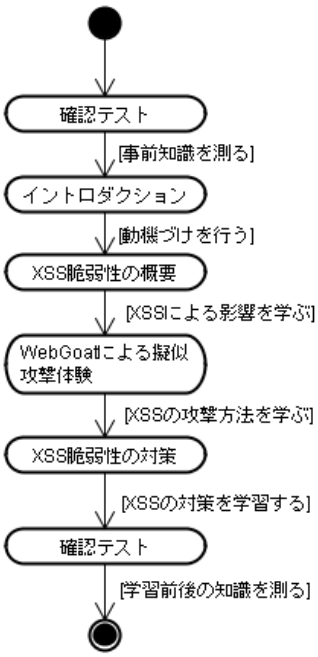

図 5　VulCES の流れ

初めにユーザの事前知識を複数の確認テストを用いて測る．事前知識が十分あると判断されたユーザは，学習しても新たに得られる知識は少ない．本来事前知識の結果によって学習するコンテンツの内容を分けるべきであるが，攻撃方法の具体的な知識を測ることは困難であったため，全員が同じ教材を学習するようにした．

次にいきなり XSS 脆弱性の説明に入る前にユーザの動機づけを行い，学習目標，使命や役割などをアニメーションの対話形式で表現した. また XSS の概要においても対話形式によるシナリオを採用したが，XSS の攻撃の流れなどイメージしづらいものは図をアニメーションにして表現した（図 6 参照）.

攻撃の流れを学習した後，WebGoat の機能を用いて XSS 脆弱性の擬似攻撃を体験し，攻撃手法を学ぶ．VulCES-XSS では WebGoat にある代表的な 2 種類の XSS レッスン「Stored XSS Attacks」および「Stored XSS Attacks」を導入した．なお，攻撃手法が判らない人向けにそれぞれヒントを 3 つ儲け，それによって攻撃手法を考察させるようにした.

XSS 脆弱性の対策については IPA が発行した“安全なウェブサイトの作り方”[6]を参考に作成した. こちらも XSS 脆弱性の概要と同じく，なるべく多く対話形式によるアニメーションを用い，必要な場合図のアニメーションを用いた.

最後に，VulCES-XSS 終了後再び確認テストを行い，学習前と学習後で得た知識を確認する．なお，学習前後の確認テストは同一のものである.

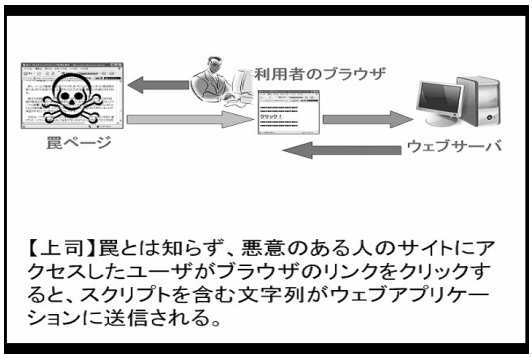

図 6　XSS の説明画面

4. 評価

4.1. VulCES-XSS の評価方法

はじめに著者らは「安全なウェブサイト運営入門」の XSS ストーリーに対し，より高い技術を持つ人向けに改良してきた[7]．本稿ではその改良システムを XSSNovel と称す. 今回の評価では，XSS 脆弱性の啓発に対し，XSSNovel および VulCES-XSS を比べ以下 7 つの項目について評価を行った.

- XSS がどういった環境において存在しうるか理解できたかどうか
- XSS 脆弱性を悪用した攻撃の仕組みについて理解できたかどうか
- XSS 脆弱性が発覚した際の対策・対処法について理解できたかどうか
- XSS 脆弱性について十分学習できたかどうか

- 学習したことは実際役立つと思うか
- WebGoat への疑似攻撃を通じて攻撃手法を理解できたかどうか
- 脆弱性を教育するにあたり，攻撃手法まで詳しく教えるべきかどうか

評価方法は東京電機大学未来科学部情報メディア学科，情報セキュリティ研究室に所属する 11 人に対しアンケート形式で調査した．また，評価結果の信憑性を高めるため評価への参加者を以下 2 つの班に分け，評価を実施してもらった．

A 班： 先に XSSNovel を学習し，後 VulCES-XSS を学習する

B 班： 先に VulCES-XSS を学習し，後 XSSNovel を学習する

被験者 11 人のうち，学習前から脆弱性に関して十分な知識を持つ人は A 班に 2 人，B 班に 2 人いた．学習前から脆弱性に関して十分な知識を持つ者を上級者とし，その他被験者を中級者とする．

4.2. 自己診断テスト

アンケートとは別に，2 つの学習システムを学ぶ前と学んだ後に自己診断テストを行い，学習効果を測った．

自己診断テストでは XSS に関する技術的な知識を選択肢形式で問いた．その内容を表 3 に示す．

4.3. 評価結果

A 班および B 班の自己診断テストの点を表 2 に，アンケート結果を表 4，表 5 に示す．

中級者の学習前のテストの平均は A 班，B 班問わず共に低かったが，学習後のテストの平均点は共に高得点だった．また，学習前から十分な知識を持つ上級者は学習前後において大きな点差は見られなかった．

表 2　自己診断テストの点の比較

	A班の平均点		B班の平均点	
	中級者	上級者	中級者	上級者
学習前のテストの点（30点満点）	12.8	17.5	9.3	19.5
学習後のテストの点（30点満点）	21.5	28.0	16.7	21.5

表 4 のアンケート結果を見ると，XSSNovel に比べて VulCES-XSS の方が全体的な理解度が高く，また VulCES-XSS の全体的な満足度も高かった．

表 5 のアンケート結果を見ると，中級者の方が上級者に比べて「コンテンツが自分に合っていた」と答える人が多く，「攻撃方法まで詳しく教えるべき」だと答えた．そのため，脆弱性への攻撃方法を知らないユーザへの学習効果はあったと考えられる．

4.4. 改善点

今回の評価アンケートで，VulCES-XSS の改善点を自由記述で書いてもらった結果，主に以下のような改善点があることが分かった．

- 画像による説明がもっと多い方が良い
- 学習するムービーが速く，全てを吸収しきれない
- 文章が長く，理解しきれない

5. おわりに

本稿では，脆弱性対策教育のための e ラーニングシステムの開発および評価について報告した．

評価結果から脆弱性を教育するにあたり，適切な防止策を理解するためには攻撃方法の理解が不可欠であることが分かった．また，e ラーニングに実践的な疑似攻撃システムを導入することで学習効果を高めていると考えられる．しかし，評価実験への被験者が少なかったこともあり，統計的な分析ができなかったことが問題である．また，アンケートからいくつかの改善点があることが分かった．

今後は VulCES が SQL インジェクションなどの他の脆弱性教育に使用できないかどうか検証しつつ，そのコンテンツも作成していきたい．

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”，http://www.ipa.go.jp/security/vuln/report/vuln2009q2.html

[2] 情報処理推進機構，“安全なウェブサイト運営入門”，http://www.ipa.go.jp/security/vuln/7incidents/

[3] ムービー塾，“DMD”，http://www.movie-school.org/

[4] 経済産業省商務情報政策局情報処理振興課，”ｅラーニング白書 2007/2008 年版”，東京電機大学出版局，2007.

[5] OWASP，“OWASP WebGoat Project“，http://www.owasp.org/index.php/Category:OWASP_WebGoat_Project.

[6] 情報処理推進機構，“安全なウェブサイトの作り方”，http://www.ipa.go.jp/security/vuln/websecurity.html

[7] 竹下数明，近藤朗，小林偉昭，佐々木良一，“サイバーセキュリティのためのゲーム的体験型学習システムの提案と評価”，コンピュータセキュリティシンポジウム 2009(CSS2009)，論文集第二分冊，pp.935-940，2008.

表 3　自己診断テストの問題

問題	選択肢の数	備考
XSSとは何か？	3	1つだけ選択
XSS脆弱性が対象なウェブアプリケーションはどれか？	3	1つだけ選択
XSS脆弱性はウェブサイト自身に影響を及ぼす。正解か否か？	2	1つだけ選択
XSS脆弱性はフォームなどで自分自身が入力する際、スクリプトを実行させないようにすれば問題は起こらない。正解か否か？	2	1つだけ選択
XSSによる脅威はどのようなものが挙げられるか？	5	複数回答
XSSの対策として全てのウェブアプリケーションに共通な対策とはどんな対策か？	4	複数回答
XSSの対策としてHTMLテキストの入力を許可しない場合の対策とはどんな対策か？	7	複数回答
XSSの対策としてHTMLテキストの入力を許可する場合の対策とはどんな対策か？	5	複数回答

表 4　両教育コンテンツの比較結果（1～4 点の 4 段階評価）

	XSSNovelの平均値	VulCES-XSSの平均値
XSSがどういった環境において存在しうるか理解できた	3.1	3.5
XSS脆弱性を悪用した攻撃の仕組みについて理解できた	2.8	3.4
XSS脆弱性が発覚した際の対策・対処法について理解できた	2.7	2.8
XSS脆弱性について十分学習できた	2.8	3.0
学習したことは実際役立つ	3.2	3.3

表 5　VulCES のアンケート結果（1～4 点の 4 段階評価）

	上級者の平均値	中級者の平均値
学習コンテンツは自分に合っている	2.8	3.1
WebGoatへの疑似攻撃を通じて攻撃手法を理解できた	3.5	2.1
脆弱性を教育するにあたり，攻撃手法まで詳しく教えるべきか	3.3	3.4