6ZC-03

脆弱性情報ハンドリング教育プログラムにおける Web サイト脆弱性体験ツールの検討

大浦 優太郎* 藤田佳菜子* 寺田 真敏*
東京電機大学

1. はじめに

IPA の 2021 年調査[1]によると，小規模な Web サイトの 23%ほどが構築時点で脆弱性対策をしていないとしている．また，Web サイトの脆弱性について知らないとするサイト運営者は，2012 年から 2020 年にかけて増加傾向にあると報告している．

Web サイトに存在する脆弱性を対策するために，国内には官民連携で運営されている情報セキュリティ早期警戒パートナーシップと呼ばれる仕組みが存在する．しかし，IPA の同調査では，『情報セキュリティ早期警戒パートナーシップの認知度』について，この仕組みについて聞いたことがない，または聞いたことはあるが内容はよく知らないと回答した Web サイト運営者が 8 割に上ると報告している．Web サイトの脆弱性を知らない，構築時点で脆弱性対策をしていないなど，脆弱性情報の取り扱い方の認知度の低さは課題と言える．

本稿では，脆弱性情報の取り扱い方の普及啓発のため，Web サイトを対象とした脆弱性情報ハンドリングを体験するための教育プログラム(以降，教育プログラム)用に開発した Web サイト脆弱性体験ツールについて報告する．教育プログラムは，脆弱性公開ポリシーの作成，脆弱性の指摘受領から対応までの体験をサポートする．Web サイト脆弱性体験ツールは，同教育プログラムを支援するため，OWASP Top 10 の脆弱性[2]を体験できる．

2. 脆弱性情報ハンドリング

2.1 情報セキュリティ早期警戒パートナーシップ

国内には IPA および JPCERT/CC が運営している情報セキュリティ早期警戒パートナーシップ[3]と呼ばれるソフトウェア製品と Web サイトの脆弱性情報の取り扱いの仕組みが存在する．Web サイトの場合，Web サイト運営者(以降，運営者)に Web サイトに存在する脆弱性の修正を促すことを目的としている．脆弱性の発見者(以降，発見者)は調整機関である IPA を通して間接的に運営者に脆弱性の存在を通知する．運営者は，IPA から受領した脆弱性情報を元に脆弱性を修正する(図 1)．また，受領した脆弱性に関連して，Web サイトから個人情報漏洩等のインシデントを確認した場合には，その事実を一般に公表する等の措置を取らなければならないとしている．

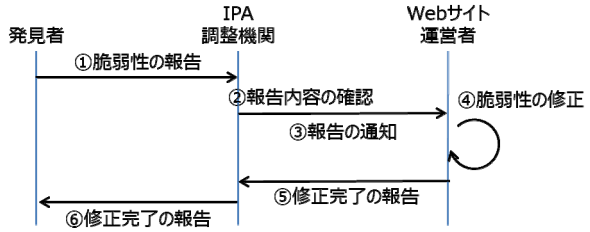

図 1 情報セキュリティ早期警戒パートナーシップにおける Web サイト脆弱性情報取り扱いフロー

2.2 OWASP Top 10

OWASP Top 10 は，Web アプリケーションのセキュリティを取り巻く課題を解決する団体 OWASP が作成している Web アプリケーションの重大な脆弱性のランキングである．このランキングは，市場の変化に合わせ数年ごとに更新されており，実際の Web サイト運営に即した内容となっている．

3. 脆弱性情報ハンドリング教育プログラム

3.1 概要

本研究では，脆弱性情報の取り扱い方の普及啓発のため，Web サイトを対象とした脆弱性情報ハンドリングを体験するための教育プログラムを検討している[5]. 教育プログラムでは，脆弱性情報取扱いフロー(図 2)そのものを体験できるように構成している．

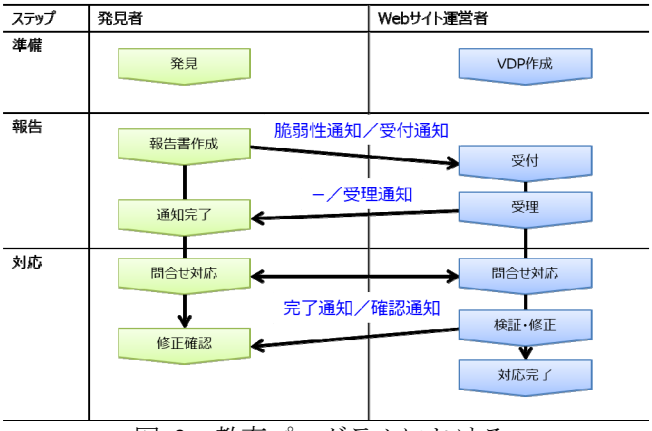

図 2 教育プログラムにおける脆弱性情報取り扱いフロー

* A Study on Web Site Vulnerability Experience Tool for Vulnerability Information Handling Education Program
Yutaro Oura, Kanako Fujita and Masato Terada Tokyo Denki University

3.2 Web サイト脆弱性体験ツールの位置付け

Web サイト脆弱性体験ツール(以降, 体験ツール)は, 発見者側では脆弱性の発見ならびに修正確認, Web サイト運営者側では検証・修正での利用を想定している. また, 実環境に近い体験環境を提供することが, 脆弱性情報ハンドリングへの理解を促すと考え, 通常の Web サイトへのアクセスと同様に, ブラウザ上で動作する体験ツールとして開発した.

3.3 体験ツール実装上の要件

Web サイトはセキュリティに関する知識を持たないユーザも利用することから, 幅広いユーザ層が教育プログラムに参加できるよう次の要件を設定し, 実装した.

- 脆弱性体験のみであれば, SaaS 型で利用できること.
  Heroku 上に体験ツールを実装することで, 教育プログラム用に環境構築を行わなくても脆弱性を体験できる.
- 脆弱性の修正を体験する場合にも, 環境構築が容易であること.
  Web サイトの脆弱性を修正する際は, 教育プログラム用に環境構築が必要となるが, 演習用資料に沿って, リポジトリのフォークとクローンで演習環境を複製後, 修正作業ができる.
- 実環境に近いものとすること.
  体験ツールで提供する Web サイトは, 画像投稿型の SNS を想定して実装した(図 3). ユーザはこのサイトに会員登録をすることによって, 画像と文章の投稿, 返信, 評価ができる.
- OWASP Top 10 の脆弱性を学習できること.
  Web サイトには, 実際に遭遇する可能性の高い OWASP Top 10 で報告されている脆弱性を配置した.
- Web アプリケーションのセキュリティ設定により脆弱性が発現すること.
  Web アプリケーションの脆弱性は, コードの問題に起因して発現する場合と, 設定の問題に起因して発現する場合がある. 体験ツールでは, OWASP Top 10 2017 で「Security Misconfiguration」がランク付けされていることを踏まえ, 設定の問題に起因して脆弱性が発現するよう実装した.

図 3 体験ツールの投稿一覧ページ

3.4 体験可能な脆弱性について

本節では, 体験ツールで実装した OWASP Top 2017[2]の 2 つの脆弱性について説明する.

(1) A2:2017-Broken Authentication

Broken Authentication は, 認証不備に起因する脆弱性で, 攻撃者が総当たり攻撃, 辞書攻撃などによって, Web サイトに不正アクセスできてしまうというものである. 体験ツールでは, 設定できるパスワードを制限していないため, 簡単で推測可能なパスワードを設定できてしまうという形で再現している.

(2) A7:2017-Cross-Site Scripting (XSS)

XSS は, 検証されていない Web アプリケーション入力データを他のユーザが閲覧することに起因して不正にスクリプト実行を引き起こしてしまう脆弱性である. ブラウザ上での不正なスクリプト実行によって, 認証情報の盗難など, 深刻な影響をもたらすことがある. 体験ツールでは, 投稿を表示する際に入力データに対してエスケープ処理をしていないため, 不正なスクリプトを挿入した場合, 投稿を閲覧したユーザ環境で不正なスクリプトが実行されてしまうという形で再現している.

4. まとめ

本稿では, 脆弱性情報ハンドリング教育プログラムに用いる Web サイト脆弱性体験ツールの実装について検討した.

Web サイト脆弱性体験ツールでは, 仮想の画像投稿型 SNS 上で, 情報セキュリティ早期警戒パートナーシップに則り, 脆弱性の発見から報告, 対応までのプロセスを体験できるよう OWASP Top 10 2017 の脆弱性を配置している.

今後は, 環境構築の簡易化, 脆弱性の種類の増加や, マニュアルの拡充によって, より実際の脆弱性情報ハンドリングに近い体験ができる Web サイト脆弱性体験ツール実装を進めていく.

参考文献

[1] IPA, “IPA 小規模 Web サイト運営者の脆弱性対策に関する調査報告書”, https://www.ipa.go.jp/files/000089536.pdf, 2022 年 1 月 2 日参照.

[2] OWASP, “2017 Top 10”, https://owasp.org/www-project-top-ten/2017/Top_10 , 2022 年 1 月 2 日参照.

[3] IPA, ”情報セキュリティ早期警戒パートナーシップガイドライン”, https://www.ipa.go.jp/security/ciadr/partnership_guide.html, 2022 年 1 月 2 日参照.

[4] 藤田佳菜子・大浦優太郎・寺田真敏, “Web サイトを対象とした脆弱性情報ハンドリング教育プログラムの検討”,情報処理学会第 84 回全国大会, 2022