各　　位

2025 年 11 月 13 日
株式会社インプレス

「安全なコードを書く力」が身につく！
『Python で学ぶ Web アプリのセキュアコーディング 脆弱性の見つけ方・直し方が身につく実践入門』を 11 月 13 日（木）に発売

インプレスグループでIT関連メディア事業を展開する株式会社インプレス（本社：東京都千代田区、代表取締役社長：高橋隆志）は、Webアプリの脆弱性の原因と対策を理解し、「安全なコードを書く力」を身につけられる書籍『Pythonで学ぶ Webアプリのセキュアコーディング 脆弱性の見つけ方・直し方が身につく実践入門』を2025年11月13日（木）に発売いたします。

■攻撃と防御を追体験しながら、Pythonで「安全なコードを書く力」を身につけられる

Webサービス開発の現場では、スピード重視のリリースが優先され、脆弱性テストやセキュリティレビューが後回しにされるケースが少なくありません。結果として、脆弱性を抱えたまま公開されるアプリが数多く存在し、情報漏洩や不正アクセスの温床となっています。

本書『Pythonで学ぶ Webアプリのセキュアコーディング 脆弱性の見つけ方・直し方が身につく実践入門』は、そうした「構造的なリスク」を正面から捉え、安全なWebアプリ開発のために何を理解し、どのように実装すべきかを、Pythonによるハンズオン形式で学べる入門書です。

セキュリティの専門家でなくても、実際の攻撃と防御のプロセスを追体験しながら、「安全なコードを書く力」を身につけられる内容となっています。

■脆弱性の「概要→攻撃→原因→対策」を体験しながら学べる構成

本書では、Webアプリで頻出する脆弱性について、それぞれ「概要」「攻撃手法」「原因」「対策」の4ステップで解説しています。各章では、SQLインジェクション、クロスサイトスクリプティング（XSS）、OSコマンドインジェクション、HTTPヘッダインジェクション、クロスサイトリクエストフォージェリ（CSRF）、パストラバーサル、XML外部エンティティ（XXE）など、実務で遭遇しやすい脆弱性を題材に、学習用アプリケーション「DSCLab（通称：やられアプリ）」を使って実際に検証できます。

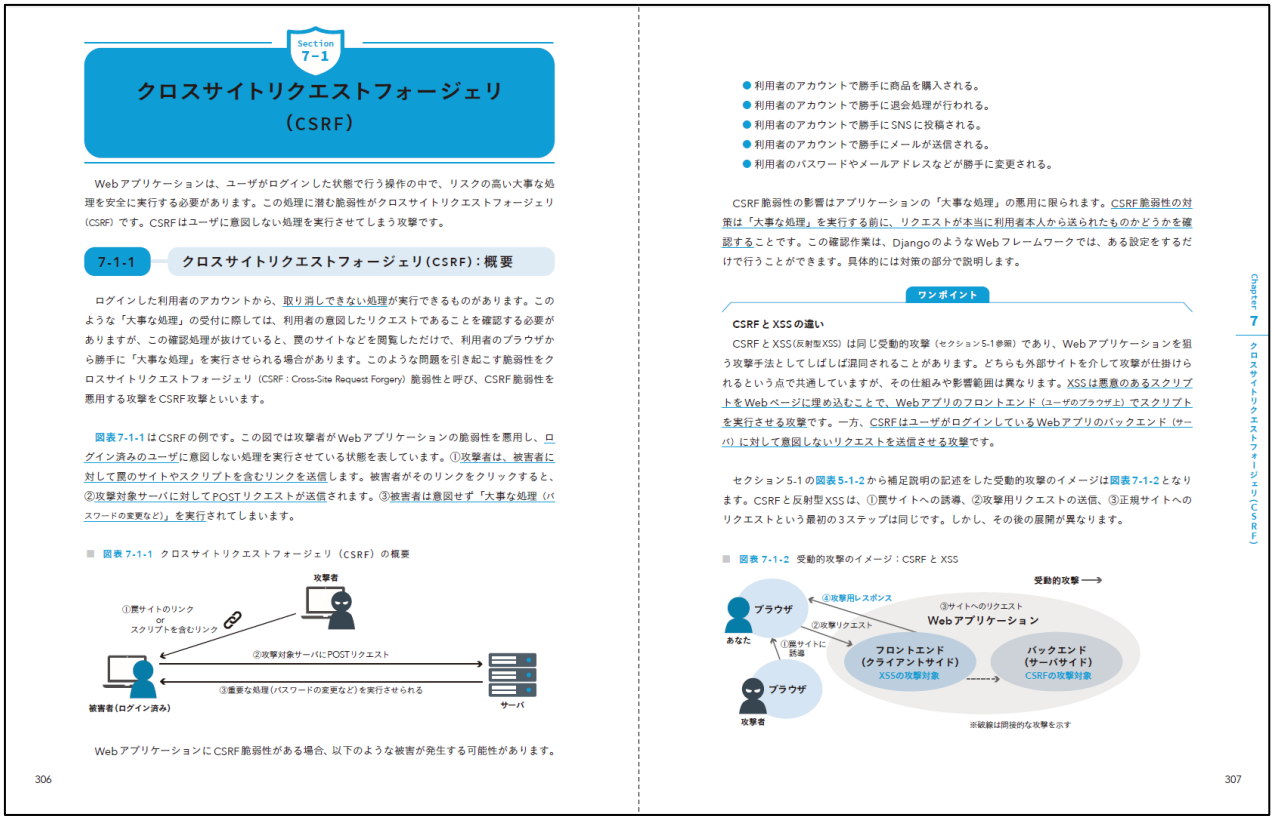
脆弱性に関する基礎知識を学べるだけでなく、「脆弱性を再現し、修正して、再テストする」体験を通して、その仕組みを深く理解できます。さらに、ライブラリの脆弱性管理（SCA/SBOM）やDocker環境での安全なセットアップなど、現場に近いトピックまで踏み込んでいます。

「なぜ脆弱性が生まれるのか」「どう直すのが最善か」を実際のコードで確かめられる、セキュリティ学習書の決定版です。

■本書は以下のような方におすすめです

- Python で Web アプリを開発しており、セキュリティ対策を実践的に学びたい方
- 新人・若手エンジニアとして、安全なコードを書くスキルを体系的に身につけたい方
- 脆弱性の「原因」と「修正方法」をコードレベルで理解したい方
- 研修・教育目的でセキュアコーディングを教える講師・指導者の方
- Web アプリ開発において、セキュリティの基礎を根づかせたいチームリーダーの方

■紙面イメージ


Section 7-1

クロスサイトリクエストフォージェリ（CSRF）

Webアプリケーションは、ユーザがログインした状態で行う操作の中で、リスクの高い大事な処理を安全に実行する必要があります。この処理に潜む脆弱性がクロスサイトリクエストフォージェリ（CSRF）です。CSRFはユーザに意図しない処理を実行させてしまう攻撃です。

7-1-1 クロスサイトリクエストフォージェリ（CSRF）：概要

ログインした利用者のアカウントから、取り消しできない処理が実行できるものがあります。このような「大事な処理」の受付に際しては、利用者の意図したリクエストであることを確認する必要がありますが、この確認処理が抜けていると、罠のサイトなどを閲覧しただけで、利用者のブラウザから勝手に「大事な処理」を実行させられる場合があります。このような問題を引き起こす脆弱性をクロスサイトリクエストフォージェリ（CSRF：Cross-Site Request Forgery）脆弱性と呼び、CSRF脆弱性を悪用する攻撃をCSRF攻撃といいます。

図表7-1-1はCSRFの例です。この図では攻撃者がWebアプリケーションの脆弱性を悪用し、ログイン済みのユーザに意図しない処理を実行させている状態を表しています。①攻撃者は、被害者に対して罠のサイトやスクリプトを含むリンクを送信します。被害者がそのリンクをクリックすると、②攻撃対象サーバに対してPOSTリクエストが送信されます。③被害者は意図せず「大事な処理（パスワードの変更など）」を実行されてしまいます。

図表7-1-1 クロスサイトリクエストフォージェリ（CSRF）の概要

Webアプリケーションに CSRF 脆弱性がある場合、以下のような被害が発生する可能性があります。

306

- 利用者のアカウントで勝手に商品を購入される。
- 利用者のアカウントで勝手に退会処理が行われる。
- 利用者のアカウントで勝手にSNSに投稿される。
- 利用者のアカウントで勝手にメールが送信される。
- 利用者のパスワードやメールアドレスなどが勝手に変更される。

CSRF脆弱性の影響はアプリケーションの「大事な処理」の悪用に限られます。CSRF脆弱性の対策は「大事な処理」を実行する前に、リクエストが本当に利用者本人から送られたものかどうかを確認することです。この確認作業は、Djangoのようなwebフレームワークでは、ある設定をするだけで行うことができます。具体的には対策の部分で説明します。

ワンポイント

CSRFとXSSの違い

CSRFとXSS（反射型XSS）は同じ受動的攻撃（セクション5-1参照）であり、Webアプリケーションを狙う攻撃手法としてしばしば混同されることがあります。どちらも外部サイトを介して攻撃が仕掛けられるという点で共通していますが、その仕組みや影響範囲は異なります。XSSは悪意のあるスクリプトをWebページに埋め込むことで、Webアプリのフロントエンド（ユーザのブラウザ上）でスクリプトを実行させる攻撃です。一方、CSRFはユーザがログインしているWebアプリのバックエンド（サーバ）に対して意図しないリクエストを送信させる攻撃です。

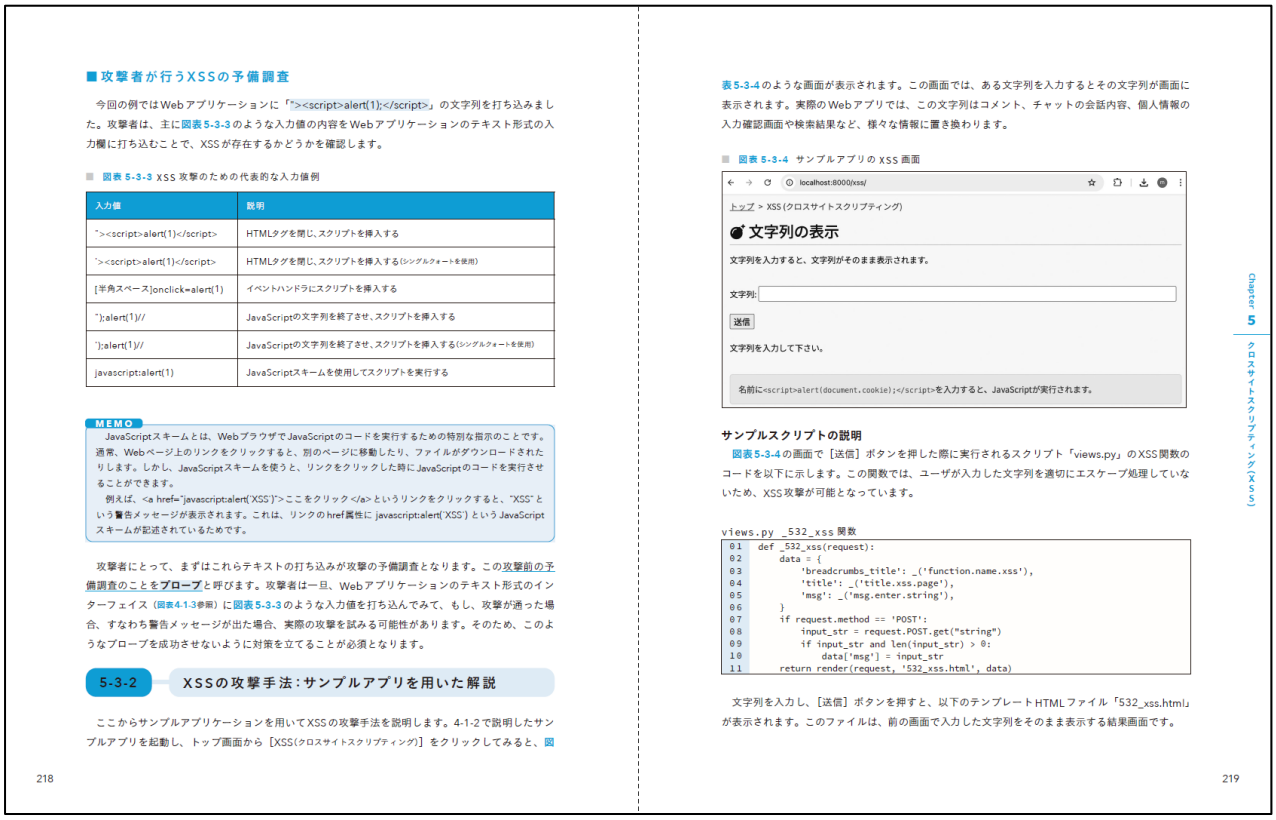
セクション5-1の図表5-1-2から補足説明の記述をした受動的攻撃のイメージは図表7-1-2となります。CSRFと反射型XSSは、①罠サイトへの誘導、②攻撃用リクエストの送信、③正規サイトへのリクエストという最初の3ステップは同じです。しかし、その後の展開が異なります。

図表7-1-2 受動的攻撃のイメージ：CSRFとXSS

307

Chapter 7 クロスサイトリクエストフォージェリ（CSRF）

各脆弱性について「概要→攻撃→原因→対策」の 4 ステップで解説。段階的に理解が深まる



■攻撃者が行うXSSの予備調査

今回の例ではWebアプリケーションに「"><script>alert(1);</script>」の文字列を打ち込みました。攻撃者は、主に図表5-3-3のような入力値の内容をWebアプリケーションのテキスト形式の入力欄に打ち込むことで、XSSが存在するかどうかを確認します。

図表 5-3-3 XSS 攻撃のための代表的な入力値例

入力値	説明
"><script>alert(1)</script>	HTMLタグを閉じ、スクリプトを挿入する
'><script>alert(1)</script>	HTMLタグを閉じ、スクリプトを挿入する(シングルクォートを使用)
[半角スペース]onclick=alert(1)	イベントハンドラにスクリプトを挿入する
";alert(1)//	JavaScriptの文字列を終了させ、スクリプトを挿入する
';alert(1)//	JavaScriptの文字列を終了させ、スクリプトを挿入する(シングルクォートを使用)
javascript:alert(1)	JavaScriptスキームを使用してスクリプトを実行する

MEMO

JavaScriptスキームとは、Webブラウザで JavaScriptのコードを実行するための特別な指示のことです。通常、Webページ上のリンクをクリックすると、別のページに移動したり、ファイルがダウンロードされたりします。しかし、JavaScriptスキームを使うと、リンクをクリックした時にJavaScriptのコードを実行させることができます。

例えば、ここをクリックというリンクをクリックすると、"XSS"という警告メッセージが表示されます。これは、リンクのhref属性に javascript:alert('XSS')というJavaScriptスキームが記述されているためです。

攻撃者にとって、まずはこれらテキストの打ち込みが攻撃の予備調査となります。この攻撃前の予備調査のことを**プローブ**と呼びます。攻撃者は一旦、Webアプリケーションのテキスト形式のインターフェイス（図表4-1-3参照）に図表5-3-3のような入力値を打ち込んでみて、もし、攻撃が通った場合、すなわち警告メッセージが出た場合、実際の攻撃を試みる可能性があります。そのため、このようなプローブを成功させないように対策を立てることが必須となります。

5-3-2 XSSの攻撃手法：サンプルアプリを用いた解説

ここからサンプルアプリケーションを用いてXSSの攻撃手法を説明します。4-1-2で説明したサンプルアプリを起動し、トップ画面から［XSS(クロスサイトスクリプティング)］をクリックしてみると、図

218

表5-3-4のような画面が表示されます。この画面では、ある文字列を入力するとその文字列が画面に表示されます。実際のWebアプリでは、この文字列はコメント、チャットの会話内容、個人情報の入力確認画面や検索結果など、様々な情報に置き換わります。

図表 5-3-4 サンプルアプリの XSS 画面

サンプルスクリプトの説明

図表5-3-4の画面で［送信］ボタンを押した際に実行されるスクリプト「views.py」のXSS関数のコードを以下に示します。この関数では、ユーザが入力した文字列を適切にエスケープ処理していないため、XSS攻撃が可能となっています。

views.py _532_xss 関数

```
01  def _532_xss(request):
02      data = {
03          'breadcrumbs_title': _('function.name.xss'),
04          'title': _('title.xss.page'),
05          'msg': _('msg.enter.string'),
06      }
07      if request.method == 'POST':
08          input_str = request.POST.get("string")
09          if input_str and len(input_str) > 0:
10              data['msg'] = input_str
11      return render(request, '532_xss.html', data)
```

文字列を入力し、［送信］ボタンを押すと、以下のテンプレートHTMLファイル「532_xss.html」が表示されます。このファイルは、前の画面で入力した文字列をそのまま表示する結果画面です。

Chapter 5 クロスサイトスクリプティング(XSS)

219

学習用アプリ「DSCLab」を使い、脆弱性の再現・修正・対策をハンズオンで学べる

■本書の構成

Chapter 1　Webアプリケーションの脆弱性の基礎
Chapter 2　Pythonサンプル（やられ）アプリのセットアップ
Chapter 3　Webアプリケーションの基礎
Chapter 4　SQLインジェクション
Chapter 5　クロスサイトスクリプティング（XSS）
Chapter 6　その他のインジェクション
Chapter 7　クロスサイトリクエストフォージェリ（CSRF）
Chapter 8　パストラバーサルとXXE、認証・認可
Chapter 9　ライブラリの脆弱性管理
Chapter 10　代表的なセキュリティテストツール
Appendix A　Dockerを使用したDSCLabのセットアップ
Appendix B　DSCLabセットアップコマンド早見表

■書誌情報

書名：Pythonで学ぶ Webアプリのセキュアコーディング 脆弱性の見つけ方・直し方が身につく実践入門
著者：森 祥平
発売日：2025年11月13日（木）
ページ数：528ページ
サイズ：B5変形
定価：3,520円（本体 3,200円＋税10%）
電子版価格：3,520円（本体 3,200円＋税10%）※インプレス直販価格
ISBN：978-4-295-02300-5

◇Amazonの書籍情報ページ：https://www.amazon.co.jp/dp/4295023000/
◇インプレスの書籍情報ページ：
https://book.impress.co.jp/books/1124101071

■著者プロフィール

森 祥平（もり・しょうへい）／Shohei Mori
東京都生まれ。電気通信大学情報工学科を卒業後、株式会社インテック（現TIS）に入社。Javaを用いた大規模ECサイトの開発に従事。その後、外資系企業にキャリアを移し、半導体企業では組み込みソフトウェア開発、マルチメディア企業ではデスクトップアプリ販売、Googleではモバイルアプリの監査を担当。
2023年よりContrast Security Japan合同会社にてソリューションアーキテクトとして、Webアプリケーションの脆弱性検出ツールIAST（Interactive Application Security Testing）をはじめとする各種ソリューションの普及に努める。2025年より行動的生体AI認証ソリューションを取り扱うBioCatch社において、ソリューションエンジニアとして技術支援を行っている。
冬場は岩原及びニセコスキー場でスキー・スノーボードインストラクターを兼務。

ビジネス・ブレークスルー大学大学院 MBA首席修了
豪州BOND University MBA（履修済み全コア科目首席）修了

以上

【本件に関するお問合せ先】
株式会社インプレス　広報担当：丸山
E-mail: pr-info@impress.co.jp URL： https://www.impress.co.jp/
※弊社はテレワーク推奨中のため電話でのお問合わせを停止しております。メールまたは Web サイトからお問合わせください。