

サイバーセキュリティ人材育成プラットフォーム

— 初学者から開発者まで —

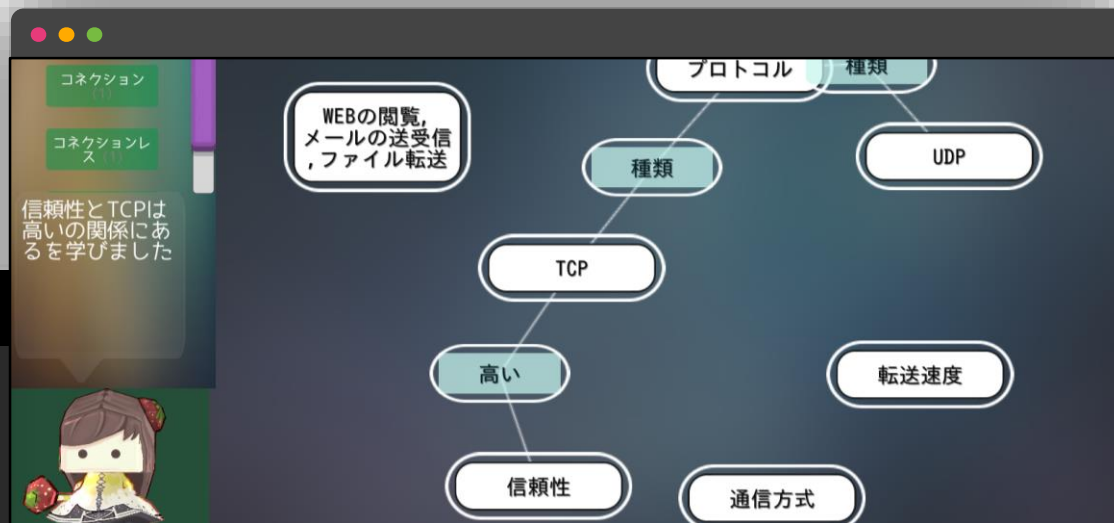
北村 拓也, 森田 浩平



Molt

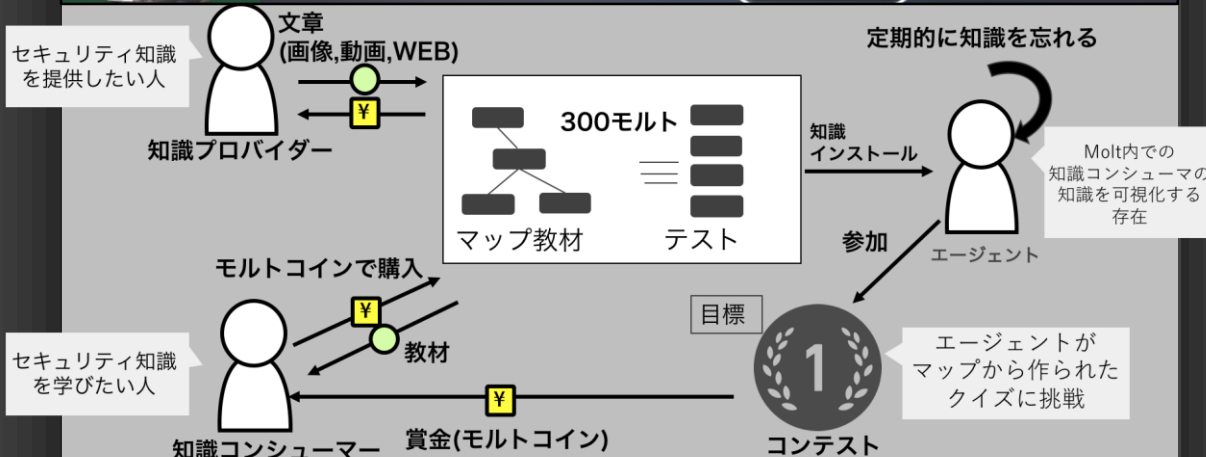
<https://molt.school/>

概念マップを
使った効率的な
学習



ユーザが
簡単に作成し
共有できる
学習コンテンツ

Teachable Agents
を用いた
モチベーション
維持の仕組み



サイバーセキュリティ人材育成プラットフォーム

— 初心者から開発者まで —

北村 拓也, 森田 浩平



<https://curevuln.com/>

Webアプリケーション
における
脆弱性の概要や
対策方法を体系的に
学べる

脆弱なアプリケーション
含め、学習コンテンツは
全てGitHubで公開
(<https://github.com/curevuln>)

クロスサイトスクリプティングとは

クロスサイトスクリプティング(XSS)脆弱性は、悪意あるユーザーが不正なスクリプトをウェブページに注入することで、その不正なスクリプトが被害者のブラウザ上で実行してしまう脆弱性です。この脆弱性が悪用されると、以下のような影響があります。

- 偽のページが表示され、フィッシングにあう
- Cookieなどの情報盗取され、漏りやすくなる

XSS脆弱性には大きく分けて以下の3種類がありますが、ここでは反射型XSSにて説明します。

1. 反射型(Reflected XSS)
2. 蓄積型(Stored XSS)
3. DOM based XSS

反射型XSS脆弱性がどのように悪用されるか以下の図をご覧ください。

```

1 <?php
2  require('common.php');
3  $ok = connectDB();
4  $query = 'SELECT * FROM item WHERE name LIKE ?';
5  $stmt = $db->prepare($query);
6
7  if (isset($_GET['name'])) {
8      $name = $_GET['name'];
9
10     $stmt->bindValue(1, '%' . addslashes($name) . '%');
11     PDO::PARAM_STR);
12     $stmt->execute();
13     $items = $stmt->fetchAll();
14     require 'template_search.php';
15 }
16 }
17

```

脆弱なアプリケーション

不正なスクリプトを含むHTMLを出力する

検索機能など第三者のウェブサイト

不正なスクリプトを含むウェブサイトを閲覧

不正なスクリプトを悪用

不正なスクリプト実行される

1. 悪意のある人が、不正なスクリプトを含むHTMLを脆弱なウェブサイトに貼り付けます。
2. 脆弱性の第三者のウェブサイト上のHTMLをクリックすることで、不正なスクリプトを脆弱なアプリケーションに実行させます。
3. 脆弱なアプリケーションは不正なスクリプトをそのままHTMLとして出力してしまいます。
4. 悪意のあるスクリプトが脆弱した被害者のブラウザ上で実行されます。

```

2018-02-28T12:04:00.527715Z # [Note] IPV6 is available.
2018-02-28T12:04:00.527748Z # [Note] 'it' resolves to '::1'
2018-02-28T12:04:00.527772Z # [Note] Server socket created on
IP: '::1'.
2018-02-28T12:04:00.530999Z # [Note] Event Scheduler: Loaded @
events
2018-02-28T12:04:00.540468Z # [Note] mysqld ready for connect
ions.
mysql: Version: '5.7.26' socket: '/var/run/mysqld/mysqld.sock' port
: 3306 MySQL Community Server (GPL)
2018-02-28T12:04:00.54052Z # [Note] Executing 'SELECT * FROM
INFORMATION_SCHEMA.TABLES; to get a list of tables using the deprecated pa
rtition engine. You may use the startup option '--disable-partition-engine-
check' to skip this check.
2018-02-28T12:04:00.540674Z # [Note] Beginning of list of non-mat
rially partitioned tables
2018-02-28T12:04:00.551872Z # [Note] End of list of non-mat
rially partitioned tables

```

脆弱性の原理から
発見、対策について
実際に試しながら
学べる

問題に挑戦して
理解度確認
自動採点による
効率的な学習を提供

Incorrect :(

```

+++ Actual
@@ @@
-'&#039;'
+''

```

`/var/www/html/check.php:51`

Connection Closed

FAILURES!
Tests: 1, Assertions: 1, Failures: 1.

• '''に変換されていません