セキュリティ・ネットワーク学実験 3(B2)
Web アプリケーション脆弱性演習

2600200087-2
Oku Wakana
奥 若菜

July 9 2022

1　クロスサイト・スクリプティング

1.1　脆弱性の概要および発見演習

1.1.1　クロスサイト・スクリプティングの概要

クロスサイト・スクリプティングの脆弱性とは、不正なスクリプトを何らかの手段で Web ページに埋め込むことで、その不正なスクリプトが被害者のブラウザ上で実行されてしまう脆弱性である。この脆弱性が利用されることで、偽の Web ページが表示されたり、Cookie が不正に取得されるといった被害が発生する。

1.1.2　脆弱性の発見手法

HTML で出力する時に「>」を「<」に置換するなど、特別な意味を持つ文字を、特別な意味を持たない表記文字に置換することをエスケープ処理と言う。受け取った入力データを、エスケープ処理を行わずに画面に出力している箇所があれば、クロスサイト・スクリプティングの脆弱性となる。

1.1.3　脆弱性の発見演習

下の図 1 のより、脆弱性のあるプログラムの名前欄に「'>"><hr>」と入力し、リクエスト送信したところ、出力画面に水平な線が表示された。また、図 2 のより、対策が行われているプログラムに同じ入力を行ったところ、入力した文字列がそのまま表示された。

図 1　脆弱性のあるプログラム

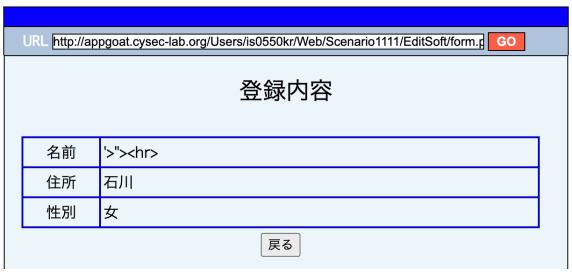

図 2　対策の行われているプログラム

これらのフレーム内のソースコードを示した図 3,4 より、脆弱性のあるプログラムでは<hr>がタグとして扱われているのに対し、対策の行われているプログラムでは、全てが文字列として扱われていることが分かる。

図 3　脆弱性のあるプログラム

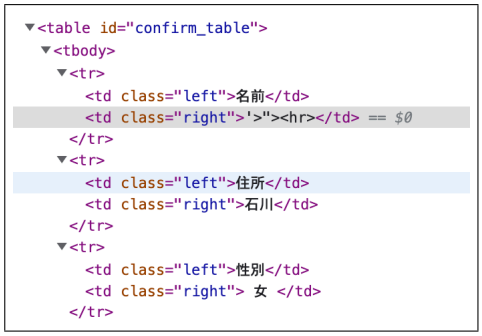

図 4　対策の行われているプログラム

1.2　アンケートページの改ざん (反射型)

反射型クロスサイト・スクリプティングの脆弱性とは、Web アプリケーションがユーザから受け取った入力データを、そのままの形（実行可能な形）でウェブページの出力に利用してしまう問題である。アンケートページの名前欄に反射型の脆弱性が発見できたため、名前欄に相当するパラメータである「name」の値にスクリプトを書き込み、作成した URL を名前欄に入力した。

下の図 5,6 はそれぞれ実行前と実行後のアンケートページの画面である。リクエストを送信することで、「*のついている項目は入力必須です。」という注意書きを書き換えることができた。

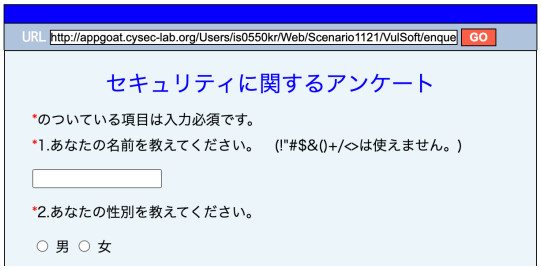

図 5　実行前の画面

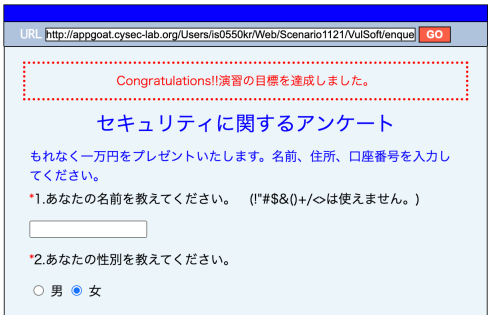

図 6　実行後の画面

1.2.1　入力情報の漏洩 (反射型)

投稿ボタンをクリックすると、ポップアップダイアログによって送信先を表示するようなアンケートページにおいて、送信先を変更するようなスクリプトを含む URL を作成し、名前欄に見つかった反射型の脆弱性を利用してスクリプトを実行させた。

下の図 7,8 はそれぞれ実行前と実行後で、表示されたポップアップをキャプチャしたものである。内容を見ると送信先の URL が書きかわっていることが確認できる。

図 7　実行前の画面

図 8　実行後の画面