単元
04

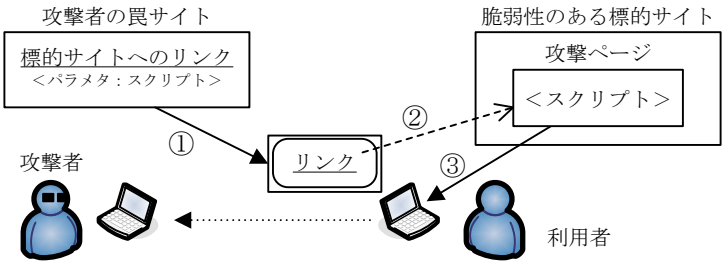
情報セキュリティ全般

Web サイト利用者への攻撃

・クロスサイトスクリプティングについて理解する
・クロスサイトリクエストフォージェリについて理解する
・Web サイト利用者に対する，その他の攻撃について理解する

クロスサイトスクリプティング（XSS：Cross Site Scripting）

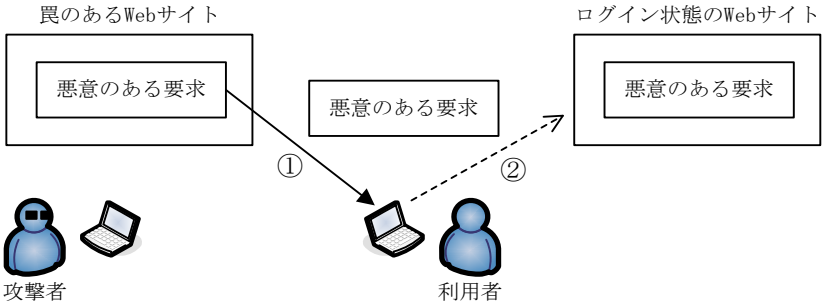
悪意をもったスクリプトを，脆弱性のある標的サイト経由で利用者に送り，その標的サイトにアクセスした利用者にスクリプトを実行させて，情報を盗み出す攻撃



① 罠サイトの閲覧などにより，標的サイトへのリンクなどを表示させる。
② クリック等によりスクリプトを含む文字列を送らせ，攻撃ページを出力させる。
③ 利用者のブラウザでスクリプトを実行させ，利用者の情報などを送信させる。

クロスサイトリクエストフォージェリ（CSRF：Cross-Site Request Forgeries）

ある Web サイトにログインした状態で，罠のある別の Web サイトにアクセスした結果，ログインしている Web サイトに悪意のある要求（リクエスト）が利用者の要求と偽って（フォージェリ）送られ，実行される攻撃



① 罠のある Web サイトから，アクセスした利用者に悪意のある要求を送り込む。
② 利用者の要求と偽って，別の Web サイトに悪意のある要求を実行させる。

関連するその他の攻撃

1) **クリックジャッキング**

利用者がログインしている Web ページを透明化して罠 Web サイトの前面に仕掛け，クリック操作を誘導して利用者の意図しない処理を実行させる攻撃

2) **セッションハイジャック**

正規のユーザが Web サイトなどと通信している最中に，セッション（特定利用者間の一連の通信群）を乗っ取る攻撃

3) **ドライブバイダウンロード**

Web サイトの閲覧時に，ユーザの許可なしに（又は，ユーザに気付かれないように）不正プログラム（マルウェアなど）をダウンロードさせる攻撃

4) **ガンブラー**

有名企業や公共機関の Web サイトを改ざんし，改ざんした Web サイトを閲覧した利用者を罠 Web サイトなどに誘導してコンピュータウイルスを感染させる攻撃

5) **ブラウザハイジャック**

Web サイトを閲覧するソフトウェア（ブラウザ）の設定の改変や，不正な機能の追加によって，利用者の望まない動作を強制的に引き起こす悪質なソフトウェア（**ブラウザハイジャッカー**）を送り込む攻撃

関連知識

攻撃者の種類

- **愉快犯**

  世間を騒がせることを目的とする攻撃者（スクリプトキディなど）

- **詐欺犯**

  相手を騙し，金銭などを奪取することを目的とする攻撃者

- **故意犯**

  自身の行為が正当でないことを理解している攻撃者

- **確信犯**

  自分の行動は正しいと信じて，**ハクティビズム**（社会／政治的な主義・主張のもとにハッキング活動を行うこと）や**サイバーテロリズム**（インターネットなどを利用した大規模な破壊活動）を行う攻撃者

  ※ハッキング：システムにアクセスして，構造解析や改変をする行為
  （悪意のあるハッキングを“クラッキング”と区別する）

問１　クロスサイトスクリプティングに関する記述として，適切なものはどれか。

ア　Web サイトの運営者が意図しないスクリプトを含むデータであっても，利用者のブラウザに送ってしまう脆弱性を利用する。
イ　Web ページの入力項目に OS の操作コマンドを埋め込んで Web サーバに送信し，サーバを不正に操作する。
ウ　複数の Web サイトに対して，ログイン ID とパスワードを同じものに設定するという利用者の習性を悪用する。
エ　利用者に有用なソフトウェアと見せかけて，悪意のあるソフトウェアをインストールさせ，利用者のコンピュータに侵入する。

問２　クロスサイトリクエストフォージェリが攻撃対象とする利用者はどれか。

ア　自身の生年月日をパスワードに設定する利用者
イ　複数の Web サイトで同じパスワードを使っている利用者
ウ　不特定多数の人が使用する PC でパスワードを入力する利用者
エ　他の Web サイトに正当なパスワードでログインした状態の利用者

問３　サーバとクライアント間の正規の通信群を乗っ取ることで，正規のクライアントになりすまし，サーバ内のデータなどを盗み出す攻撃はどれか。

ア　クリックジャッキング　　イ　セッションハイジャック
ウ　ドライブバイダウンロード　　エ　ブラウザハイジャック

解説・解答　8ページ

科目 B

問4 次の記述中の [a] , [b] に入れる正しい答えの組合せを，解答群の中から選べ。

N社は，インターネット上で日用雑貨品の会員制通信販売システムを運営する会社である。また，N社では，情報交換の場として，会員以外の人でも利用できる掲示板システムを提供している。

N社の掲示板システムは，入力された文字列にエスケープ処理を適切に施してから，ブラウザに表示するように設定されている。このエスケープ処理では，HTML の特別な記号文字“<”，“>”，“&”などを，それぞれ“<”，“>”，“&”といった別の表記方法に置き換える。このエスケープ処理を行うと，文字列“<script>”は文字列“ [a] ”に置き換えられる。このように，入力された文字列にエスケープ処理を施すようにしている理由は，悪意のあるコードを [b] ためである。

解答群

	a	b
ア	>script<	埋め込まれたページを削除する
イ	>script<	投稿された時点で検出する
ウ	<script>	投稿した人を特定する
エ	<script>	ブラウザで実行させない
オ	>script<	埋め込まれたページを削除する
カ	>script<	投稿された時点で検出する
キ	<script>	投稿した人を特定する
ク	<script>	ブラウザで実行させない

解説・解答　9ページ