XSS　クロスサイトスクリプティング

XSS(クロスサイトスクリプティング)とは

Webアプリの脆弱性を利用して悪意のあるデータを埋め込み、スクリプトを実行させる攻撃のこと

試してみよう

掲示板に投稿

書き込むBoxに文字を書き込んで投稿すると掲示板に書き込まれます

どうやらWebブラウザーが理解できる言葉を使うと良くないことが出来そう

```
<img src="1" onerror="alert(1)">
```

EXマンボタンを押してもヨシ（挙動は少し違う）

SQLインジェクション

SQLインジェクションとは

Webアプリの脆弱性を利用して

データベースを不正に操作する攻撃のこと

試してみよう

見れないはずのすべてのデータを取得

製品名の検索蘭には何も検索しないか、「テスト」「テ」「ス」「ト」「テス」など検索したものに関連するデータが表示される

これもデータベースと呼ばれるデータを保存するシステムが理解できる言葉を使うと何やら悪いことができそう

```
1' or '1' = '1'%3B--
```

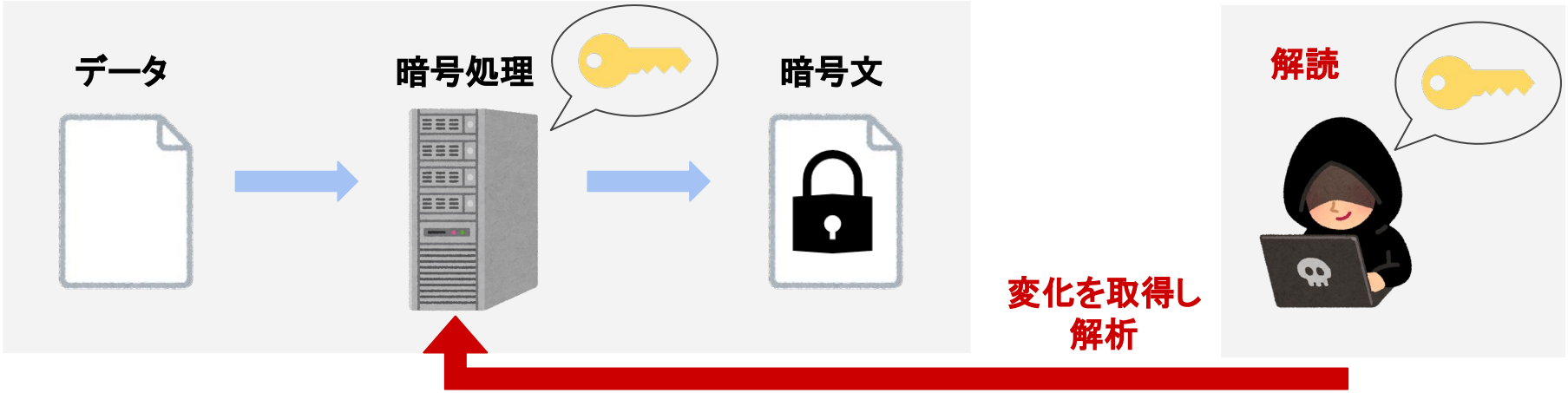
他にも刺さる文があるかも

サイドチャネル攻撃

サイドチャネル攻撃とは

暗号処理を行っているコンピュータの特徴を

観察・測定することで内部情報を取得する攻撃のこと



タイミング攻撃

コンピュータに命令を送り、命令処理の時間差を分析して情報を盗む攻撃

具体例

パスワードが「kanazawa」だった場合、

1文字目に「k」を入力した時だけ応答時間が長かった

→ 1文字目のパスワードは「k」と判断できる

クイズ

あるWebサイトのログインフォームには、サイドチャネル攻撃が可能です。

どうやら名前とパスワードで認証する仕組みのようですが、ITに関連のある有名人の下の名前とそれに関連するモノのパスワードを設定しているようです。

今回のセキュリティの穴

F12を押すと開発者モードに変わるネットワークを開こう

開いたまま名前とパスワードを入力してログインボタンを押すと応答にかかった時間が分かる

・どうやらユーザーが存在している時としていないときの時間が違う

・返ってくるメッセージもかなり具体的

・番号が違う

サービスを利用しているユーザーが誰か分かってしまう！

ヒント（ここに出ている大文字以外は全部小文字です）

B〇〇l (4)　M〇〇〇〇〇〇〇t (9)　創設者　Windowsを作った会社

S〇〇〇shi (7)　B〇〇〇〇〇n (7)　日本人？仮想通貨の生みの親　仮想通貨の名前

S〇〇〇e (5)　〇P〇〇〇n (6)　🍎📱スマホといえばみたいなとこある

A〇〇n (4)　eni〇〇〇 (6)　ドイツの暗号機と解読した人

Li〇〇s (5)　li〇〇x (5)　🐧オペレーティングシステムと開発した人

Yu〇〇〇〇ro ()　r〇〇〇 (4)　日本発プログラミング言語(宝石の名前)と開発した人

L〇〇a (4)　ry〇〇〇 (5)　CPUの会社Intelではない　女性CEO

J〇〇n (4)　per〇〇〇〇〇com〇〇〇〇r (16)　IQ300!? コンピューターが進化して今

Ke〇〇n (5)　shi〇〇〇〇ra (9)　元ハッカー(クラッカー)　相対したのは日本人

もしかして、こんな風に思いましたか？

現実世界はこんなクイズみたいなのはありえない！

実際どうなの？？

パスワードの流出

実際にいろんな方法で流出したパスワードは公開されている

因みに2021、2020年

ランキング順位	日本人の漏洩パスワード		
	2021年	2020年	NordPass 2021年
1位	123456	123456	password
2位	password	password	123456
3位	000000	asdfghjk	123456789
4位	1qaz2wsx	12345678	12345678
5位	12345678	123456789	1qaz2wsx
6位	123456789	asdasd456	member
7位	111111	111111	asdfghjk
8位	sakura	1qaz2wsx	12345
9位	dropbox	19980621	password1

ちなみに45位は
doraemon

ITmediaNEWS 21年に漏えいした日本のパスワード、2位は「password」 1位は？　ソリトンシステムズ調査

漏れたメールアドレスとパスワードの行く先

今回は**名前**でしたが、よくログインの際には**メールアドレス**と**パスワード**が使われていませんか？

仮に昔、何かのサイトで利用していた認証情報が流失していて

現在使用している別のサイトでも**同じメールアドレス、使用したことのあるパスワード**を使っていたらどうでしょう？

情報は知らず知らず共有されており**リスト化**されています

攻撃者はそのようなリストを用いて、**力づくで突破**してきます

わたしたちがセキュリティを学ぶわけ

他にも多くのセキュリティ観点が単純なログイン機能に**存在**する
攻撃は一つで終わりではなく複数のものを鎖のように繋げていく

使う側ではなく作る側はどう**堅牢**なシステムをつくれば良いのか
攻撃方法を知らなければ守ることは不可能です

あなたも「セキュリティ」学びませんか？