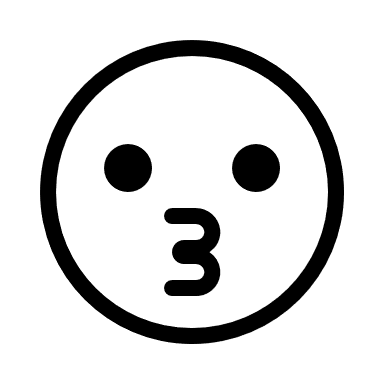
**サイバー攻撃**

**パスワードクラッキングとは**

個人情報を狙い、IDとパスワードによる認証を行う会員制Webサービスからユーザのパスワードを抜き出そうとする攻撃

何回か連続してログインに失敗したときはそのユーザの利用を停止するといった対策や、パスワードの長さを設定したり記号の入力を必須にしたりするなど、簡単なパスワードに設定できないようにするという対策が有効

・辞書攻撃…よくパスワードに使われる単語をまとめたファイルを用意して、それを使って次々と試すことでパスワードを当てる攻撃



よく使われるパスワードの一覧を試す

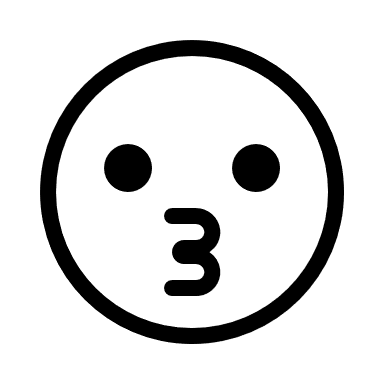
辞書ファイル

password

123456

abcdef

・ブルートフォース攻撃…パスワードに使われる文字の全組み合わせを試す方法

  
  
  
  
  
  
**Dos(Denial of Service)攻撃**

パスワードに使われる文字のパターンをしらみつぶしに試す

00000001

00000002

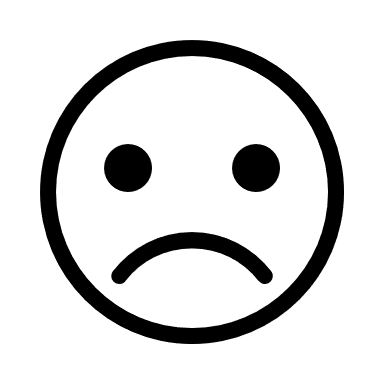
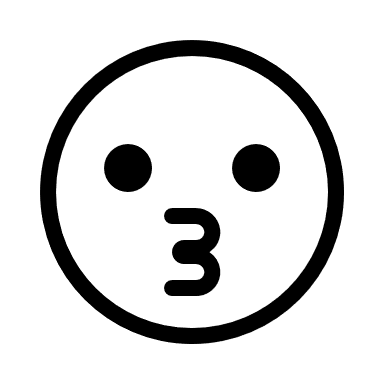
00000003

短時間にサーバが処理しきれないような大量のアクセスを行うことで、サービスの停止に陥らせる攻撃

不自然なアクセス増加を検知し送信元のIPアドレスからのアクセスをいち早く遮断するなどの対策が必要

大量のクライアントから一斉にDos攻撃を仕掛けるDDos(Distributed Dos)攻撃も存在する

・SYN Flood攻撃…TCPのやりとりにおけるSYNパケットのみを大量に送り付け、サーバを接続待ち状態にすることで、別のユーザからの新たな接続を確立できなくする攻撃



サーバが新しいSYNパケットに対応できなくなり、別のユーザがアクセスできなくなる

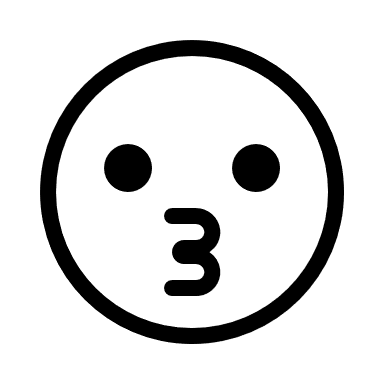
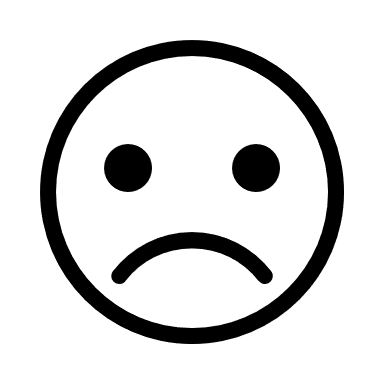
SYNパケットだけを大量に送る

SYNパケット

SYN/ACKパケット

SYNパケット

・F5攻撃…繰り返しアクセスを続けることでリクエストへの反応ができないレベルまでWebサーバの負荷を高める攻撃



大量のリクエストが来るため高負荷となる

ページの再読み込み

ページの再読み込み

Webページの要求

Webページの再読み込みリクエストを大量に送る

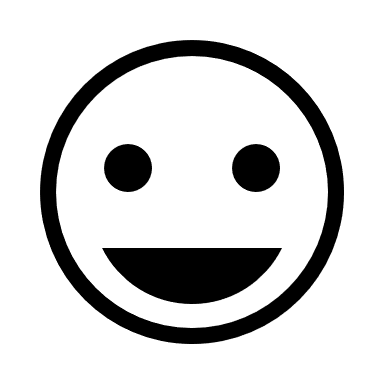
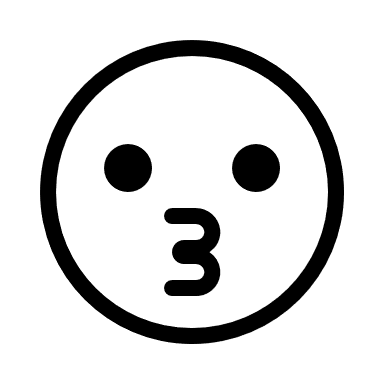
サーバのレスポンスが遅くなったり返ってこなくなる

**セッションハイジャック**

何らかの手段で第三者がCookieの中身やセッションIDを取得し、その情報を使ってログイン済みユーザとしてシステムを利用し個人情報を取得すること

CookieやセッションIDを取得する方法としては、ネットワークの盗聴やWebアプリケーションの脆弱性を突くなどの方法がある

対策として、通信を暗号化したりログインしたユーザが急に異なるIPアドレスから接続してきた場合に強制的にログアウトさせるといったつくりにしておくことが有効

  
  
  
  
  
  
  
**ディレクトリトラバーサル**

ユーザID、パスワード

セッションIDの発行

aaa012



Webサーバ

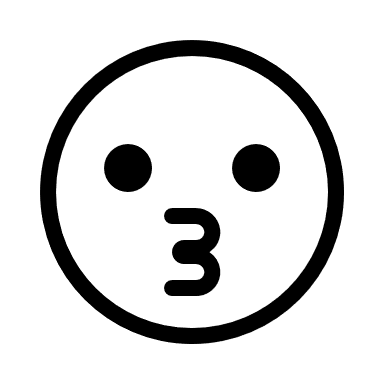
aaa012リクエスト

盗聴

セッションID「aaa012」があるからこれはAさん

Webで公開されていないディレクトリにアクセスすることでWebサーバ自体のログインパスワードを取得し、Webサーバへ不正にログインするなどの攻撃につなげること

リクエストに含まれるURLのチェックを行い、公開していないファイルが指定されていないか確認することで防ぐことが可能



Web公開ディレクトリより上の階層へたどっていき

公開されていないファイルを送信させる

GET …/…/password

password



Webサーバ

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

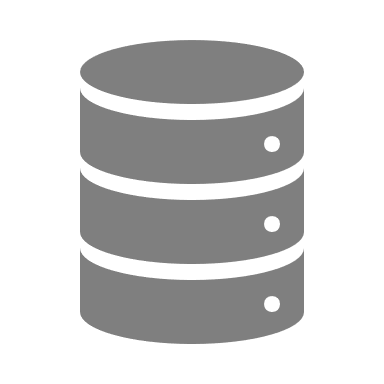
掲示板サイトのような、ユーザの入力内容を表示するタイプのWebサイトの脆弱性を突く攻撃

送り込まれるスクリプトとしては、セッションハイジャックのためのCookie情報を公開するものや、ウイルスをダウンロードするものが考えられる



悪意のあるサイト

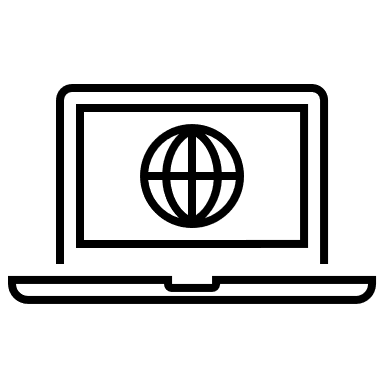
⓸



掲示板サイト

⑤

⑥



Webブラウザ

③

②②

1. 悪意のあるスクリプトを自動的に掲示板に書き込んでしまうリンクを表示する
2. 悪意のあるサイトの①のリンクにアクセスする
3. 悪意のあるスクリプトを掲示板に書き込むクライアントサイド・スクリプトが送られる
4. 意図せず悪意のあるスクリプトを書き込んでしまう
5. ユーザから送信された書き込み内容をそのまま表示
6. 掲示板に表示された悪意のあるスクリプトが実行される

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

本人になりすましてログインの必要なサイトを操作する攻撃

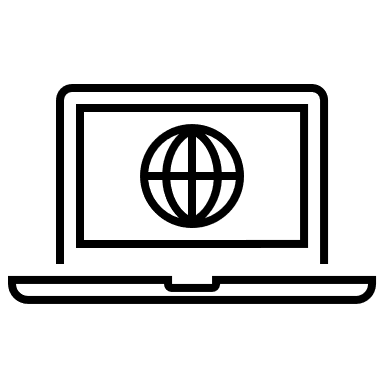
ユーザのパスワードを攻撃者の指定するものに変えたり、XSSのための悪意のあるリンクを投稿することなどが考えられる

重要な操作の場合は人の手によるアクセスかどうかを確認することで予防できる

コメントの公開範囲変更

パスワードの変更

コメントの投稿 etc

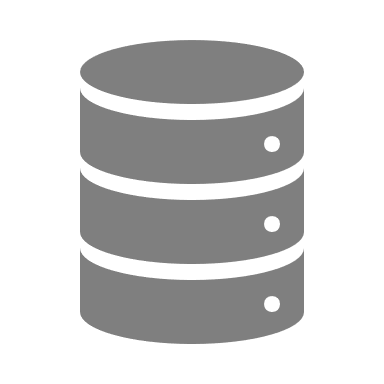


Webブラウザ

⓸



悪意のあるサイト



SNS

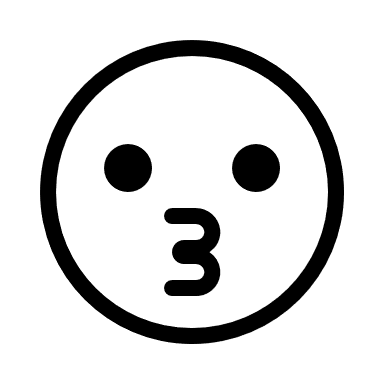
③

②②

1. SNSなどに対して操作を行うようなリンクを表示する
2. 悪意のあるサイトの①のリンクにアクセスする
3. SNSの操作を行うクライアントサイド・スクリプトが送られる
4. 事前にSNSにログインしていなければ、本人の意図しない操作を行ってしまう

**SQLインジェクション**

ユーザから送信する情報にDBが解釈できる内容を混ぜ込むことで、DBに意図しない動作を行わせる攻撃



ログインの照会の際に必ず正しいと判定される語句をパスワードとして送信

ユーザから送信された内容をそのまま利用して問い合わせ

taroのパスワード=

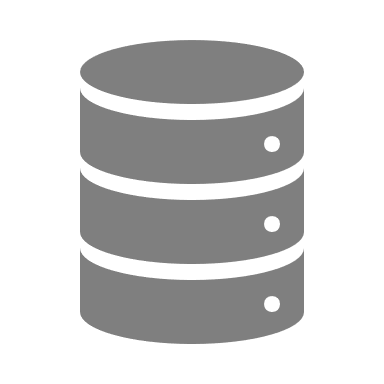
aaa or “1+1=2” ?

正しい

ユーザID→taro

パスワード→aaa or “1+1=2”

ログイン



DBサーバ



Webサーバ