**Detectarea Vulnerabilităților XSS**

**State of the Art**

1. **Introducere în Vulnerabilitățile XSS:**

Cross-Site Scripting (XSS) reprezintă una dintre cele mai frecvente vulnerabilități de securitate web, care permite atacatorilor să injecteze cod malițios în paginile vizitate de alți utilizatori. Impactul acestor atacuri poate varia de la furtul de date la preluarea completă a conturilor utilizatorilor.

2. **Tehnici Tradiționale de Detectare a XSS**:

Metodele tradiționale de detectare a vulnerabilităților XSS includ:

**Revizuirea manuală a codului**: Analiza manuală a codului sursă pentru a identifica punctele vulnerabile.

**Analiza statică**: Utilizarea unor instrumente automate pentru a analiza codul sursă fără a-l executa.

**Metode bazate pe semnătur**i: Detectarea tiparelor de atac cunoscute prin compararea acestora cu o bază de date de semnături.

Aceste metode au limitări semnificative, inclusiv rate mari de false pozitive și dificultăți în detectarea atacurilor necunoscute sau emergente.

3. **Utilizarea Machine Learning pentru Detectarea XSS**:

Aplicarea tehnicilor de machine learning pentru detectarea XSS oferă avantaje considerabile, cum ar fi capacitatea de a învăța din date și de a se adapta la noi tipare de atacuri. Modelele de machine learning pot fi antrenate să recunoască atât tiparele cunoscute de atac, cât și să detecteze anomaliile care ar putea indica atacuri noi.

4. **Progrese Recente în Detectarea XSS Utilizând Machine Learning**:

Recent, cercetătorii au explorat diverse modele de machine learning pentru a îmbunătăți detectarea XSS:

* **Arbori de decizie**: Ofertă claritate și interpretabilitate, dar pot fi susceptibili la overfitting.
* **Mașini cu vectori de suport (SVM)**: Eficace pentru seturi de date cu dimensiuni mari și oferă performanțe bune.
* **Rețele neuronale**: Capacitatea de a învăța reprezentări complexe ale datelor, dar necesită resurse computaționale semnificative.
* **Naive Bayes**: Simplu și rapid, dar poate avea performanțe slabe în fața datelor complexe și nelineare.
* **K-Nearest Neighbors (KNN)**: Ușor de implementat, dar poate deveni ineficient pe seturi de date mari.
* **Random Forest**: Oferă robustețe și performanță bună prin combinarea mai multor arbori de decizie.

5. **Provocări Cheie și Direcții Viitoare**:

Provocările actuale în aplicarea machine learning pentru detectarea XSS includ:

* **Calitatea și volumul datelor**: Necesitatea unor seturi de date diverse și bine etichetate.
* **Selecția caracteristicilor**: Identificarea celor mai relevante caracteristici pentru modelele de machine learning.
* **Costurile computaționale**: Antrenarea și rularea modelelor complexe poate necesita resurse semnificative.
* Direcțiile viitoare de cercetare includ îmbunătățirea robusteței modelelor, integrarea detectării în timp real și combinarea cu alte sisteme de securitate pentru a oferi protecție holistică împotriva atacurilor XSS.

6. **Referințe Cheie**:

Unul dintre articolele esențiale în acest domeniu este "Towards a High Coverage of Security Analysis for Web Application", care poate fi accesat la IEEE Xplore.

<https://ieeexplore.ieee.org/document/6200193>

Introducere

În această lucrare de disertație, mi-am propus să dezvolt un sistem de detectare a vulnerabilităților Cross-Site Scripting (XSS) utilizând algoritmi de machine learning. Atacurile XSS reprezintă o problemă majoră de securitate pentru aplicațiile web, permițând atacatorilor să injecteze cod malițios în paginile vizitate de alți utilizatori. Această vulnerabilitate poate duce la furtul de date, compromiterea conturilor utilizatorilor și alte consecințe grave.

Am ales această temă datorită relevanței și gravității problemei în contextul securității cibernetice moderne. Cu un număr tot mai mare de aplicații web utilizate zilnic, protejarea acestora împotriva atacurilor XSS este esențială pentru asigurarea integrității și confidențialității datelor utilizatorilor. În plus, soluțiile tradiționale de detectare a atacurilor XSS prezintă limitări semnificative, ceea ce creează o oportunitate pentru aplicarea tehnicilor avansate de machine learning.

### **Sumar al Proiectului**

În această lucrare, am implementat un sistem de detectare a vulnerabilităților XSS prin următoarele etape:

1. Preprocesarea și Vectorizarea Datelor:
   * Am utilizat modelul Doc2Vec pentru a transforma datele textuale în vectori numerici. Aceasta permite reprezentarea secvențelor de text într-o formă numerică, adecvată pentru antrenarea modelelor de machine learning.
2. Antrenarea Mai Multor Modele de Machine Learning:
   * Am antrenat și evaluat mai mulți algoritmi de machine learning pentru detectarea XSS, inclusiv Decision Tree, SVM, GaussianNB, KNeighbors, RandomForest și MLPClassifier. Fiecare model a fost antrenat pe un set de date etichetate pentru a învăța să distingă între inputurile XSS și non-XSS.
3. Evaluarea Performanței:
   * Am calculat metrici de performanță precum acuratețea, precizia, recall-ul și F1-score pentru a compara eficiența fiecărui model. Modelele au fost validate pe un set de date de test pentru a verifica capacitatea lor de generalizare.
4. Salvarea și Încărcarea Modelelor:
   * Modelele antrenate au fost salvate pe disc pentru a putea fi reîncărcate și utilizate ulterior. Aceasta permite aplicarea modelelor în medii de producție fără a fi necesară reantrenarea acestora.
5. Predicția și Clasificarea Inputurilor Noi:
   * Modelele au fost utilizate pentru a clasifica noi secvențe de input ca fiind XSS sau non-XSS. Am implementat o metodă de ponderare pentru a combina predicțiile fiecărui model, obținând astfel o decizie finală mai robustă.
6. Analiza și Validarea pe Seturi de Date Diverse:
   * Intenționez să efectuez o analiză suplimentară pe seturi de date create de mine și pe seturi de date oficiale disponibile online. Aceasta va include evaluarea modelelor pe date reale și compararea rezultatelor obținute.

Rezultatele obținute au demonstrat eficiența abordării propuse, modelele de machine learning reușind să identifice corect majoritatea atacurilor XSS. ceste rezultate evidențiază distribuția predicțiilor pentru inputurile de test, oferind o imagine de ansamblu asupra performanței modelelor.

Prin această lucrare, am contribuit la îmbunătățirea detectării vulnerabilităților XSS, propunând o metodă bazată pe machine learning care poate fi integrată în sisteme de securitate existente pentru a proteja aplicațiile web împotriva acestui tip de atac.