敵対的XSS攻撃に関する研究

Research on adversarial XSS attacks

四方 隆之介・暗号分科会・情報セキュリティ大学院大学

背景	• 敵対的XSS攻撃とはML/DLベースを避けるように設計された攻撃
先行研究	• 強化学習を用いたXSS検知モデルを回避する敵対的サンプルを生成するモデル。 • GANを使用して、LSTMベースのXSS検知モデルに対する敵対的攻撃を自動生成するアプローチの開発
課題	• 実環境での有効性検証 • 生成モデルの精度向上