WAFテストに関する研究

Research on WAF testing

髙橋 モハマドシャールク・暗号 認証分科会・情報セキュリティ大学院大学

背景

- 近年WAF(Web application firewall)を回避する攻撃の高度化が進む
- WAFの回避を未然に防ぐため、WAFの脆弱性を洗い出すWAFテストが重要視されている

先行研究

- 以下の3種類のアプローチがある
- 変異的WAFテスト：ペイロードの特定部分を変化させ、回避ペイロードを生成
- 探索的WAFテスト：回避する可能性のあるペイロードを優先的に生成
- 生成的WAFテスト：GPTを用いて、回避ペイロードを生成

課題

- 回避ペイロードの有用性がわかりにくい
- 回避ペイロードが行う攻撃のほとんどがSQLiである

今後の予定

- 攻撃シナリオを考慮したWAFテストの実現可能性を調査