# Reading Research Papers

Mohsin Sajjad
Registration No: 22PWCSE2149

**Main Contribution**

This part tells us what the research has done or created. It shows the main idea or result, like a new tool, method, or solution.

**Limitation**

This section shows the boundaries or weaknesses of the research. It tells us what the paper doesn't cover or where it might not work well.

## Paper 1: *RAXS: An Expert System for Rating Vulnerabilities*

**Author:** Jong Qianjun

**Main Contribution**

This project introduces RAXS, a system made to help beginner security analysts with the important task of checking how serious website security problems are. It uses expert knowledge, collected from professionals and trusted sources, and puts it into a set of rules. These rules help the system guide users step-by-step in judging the risk level of common web issues listed in the OWASP Top 10 (2013). This makes it easier to get expert-level advice, even when no expert is available.

**Limitations**

RAXS is limited because it only works for one part of the security check (risk assessment) and only for the OWASP Top 10 problems from 2013. Since new types of web threats keep coming up, the system needs regular updates. If it's not updated with new rules and examples, its advice will become outdated and may not help with newer problems.

# Paper 2: *Pretending to be a VIP! Characterization and Detection of Fake and Clone Channels on Telegram*

**Author:** Massimo La Morgia

## Main Contribution

This research focuses on the problem of fake and copycat (clone) channels on Telegram. The authors collected a huge amount of data — over 120,000 public channels and 247 million messages — to study how some channels pretend to be famous people or services. They grouped these into two types: fake channels, which post their own messages while pretending to be someone else, and clone channels, which copy content from real channels. To help find these fake channels, the researchers built a machine learning model that can detect them with 85.45% accuracy (F1-score). They also discovered that many of these channels are used to spread political messages, sell things, or trick people. As part of their work, they created and shared a large dataset called TGDataset to help other researchers study Telegram.

## Limitations

While the study is very useful, it has some limits. First, the model was trained using a small and manually checked dataset, so it might not work well on all types of fake channels, especially new or tricky ones. The model mainly looks at English-language channels, so it might not work as well on channels in other languages. Also, the study doesn't track how fake channels change or grow over time. It doesn't fully test what might happen if the model is used in real life, like whether it might wrongly label a real channel as fake. Lastly, the paper doesn't suggest clear solutions for how Telegram can stop or reduce fake channels in the future.