JAAM: Web Browser Security Framework

Final Presentation, April 2019
Minor Project (CSE-329)
MANIT, Bhopal (India) 462003

Outline

- About Project
- About Team
- Proposed Work
- Browser Attack Scenarios
- JAAM: Web Browser Security Framework
- Malicious URL detection tool
- Results
- References

About Project

- So called “minor” project; not actually minor!
- No innovation expected, elements of research required
- Hands-on theoritical and practical contributions
- *Delieverables:* Report, Presentation, Code, etc.
- Preparation of a paper based on project; project paper
- No. of credits: 2

About Team

- Team members:

– Jishan Shaikh	(161112013)	CSE-1
– Ankit Chouhan	(161112051)	CSE-1
– Ankit Chaudhary	(161112048)	CSE-1
– Mansoor Sediqi	(161112101)	CSE-1

- Supervisor:
  - Dr. Deepak Singh Tomar (Dept of CSE, MANIT Bhopal)
- Reviewers and Co-ordinators:
  - Dr. Rajesh Wadhvani (Dept of CSE, MANIT Bhopal)
  - Dr. Sanyam Shukla (Dept of CSE, MANIT Bhopal)

Proposed Work

- Theoritical works
  - JAAM: Web browser security framework
    - Component based framework focus on security
    - Design, Tools & Applications, Code utilities, Miscellaneous components
  - Study of modern web browsers security practices
- Practical works
  - Malicious URL detection tool (Under Tools & Applications)
    - Using Binary univariate logistic regression

Browser Attack Scenarios (1 of 2)

- Most common browser attacks*
  - Injection
  - Broken authentication
  - Broken access control
  - Cross Site Scripting (XSS)
  - Insufficient logging
  - Man in browser attack

**Source: OWASP's Top Ten Vulnerabilities 2017*

Browser Attack Scenarios (2 of 2)

- Injection attacks and Cross Site Scripting (XSS)
  - e.g. SQL injection, URL scripting
- Man in browser attack:
  - e.g. Client side attack by hackers
- Denial of Service and Distributed Denial of Service
  - e.g. Botnets, Buffer overflows
- Phishing
  - e.g. Social engineering attacks

Web Browser Security Framework (1 of 4)

- Based on 4 basic components
- Design component
  - Web Browser Security Assurance Maturity Model (WBSAMM)
- Tools and applications component
  - Malicious URL detection tool
- Code utilities component
- Miscellaneous component
  - Cheat sheets on Browser attacks and their mitigations

Web Browser Security Framework (2 of 4)

Features of the framework:

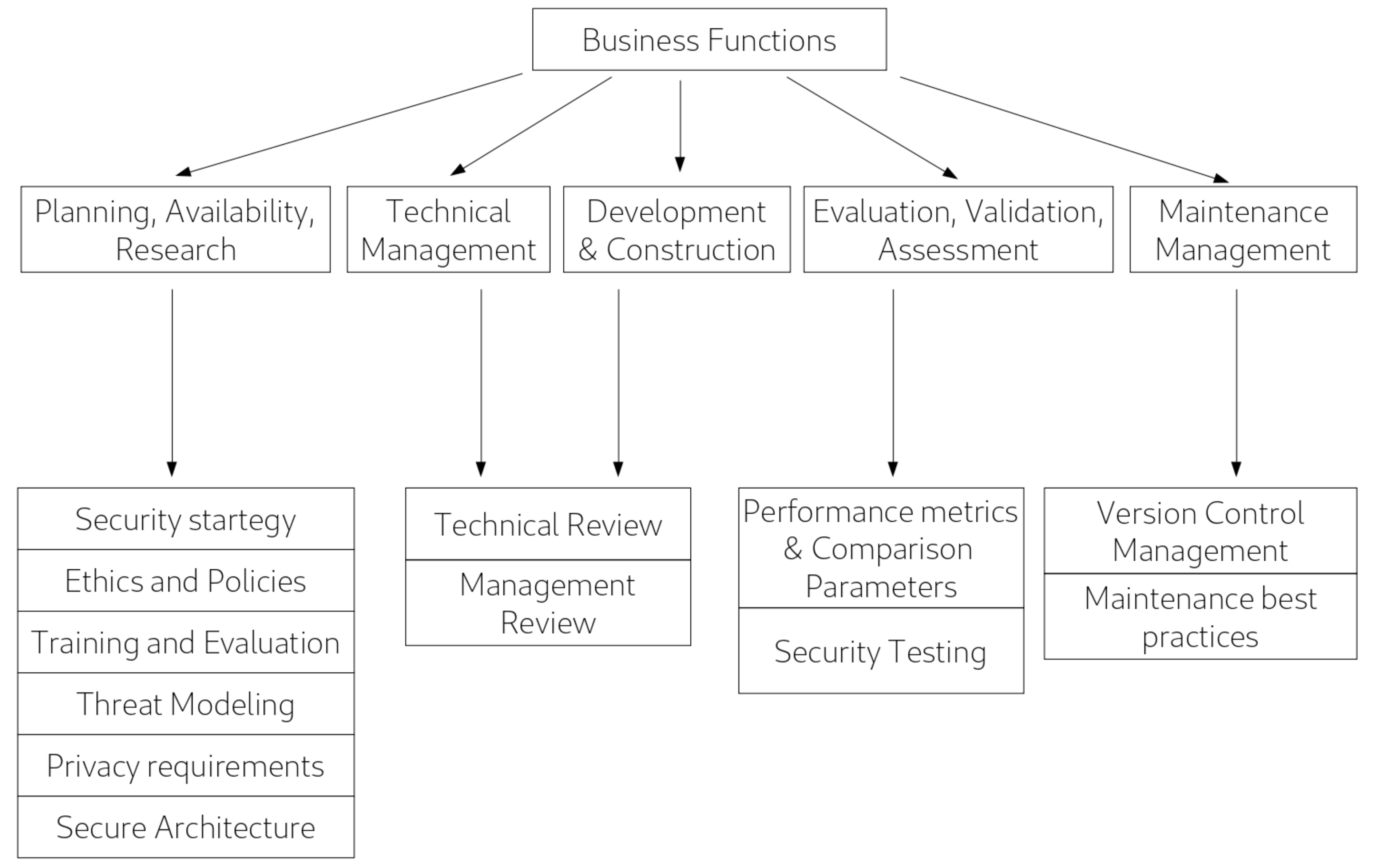
- Adaptive to all scale organizations (Small, Medium, Large)
- Easy customization
- Neutral towards life-cycle models
- Open Source
- Standardization of security practices for web browsers

Web Browser Security Framework (3 of 4)

Security Assurance Maturity Model:

- Based on
  - Business Functions
  - Security Practices
  - Maturity Levels (1 to 10)
- Architecture diagram (.....Continued)

Web Browser Security Framework (4 of 4)



Business Functions

Planning, Availability, Research

Technical Management

Development & Construction

Evaluation, Validation, Assessment

Maintenance Management

Security startegy

Ethics and Policies

Training and Evaluation

Threat Modeling

Privacy requirements

Secure Architecture

Technical Review

Management Review

Performance metrics & Comparison Parameters

Security Testing

Version Control Management

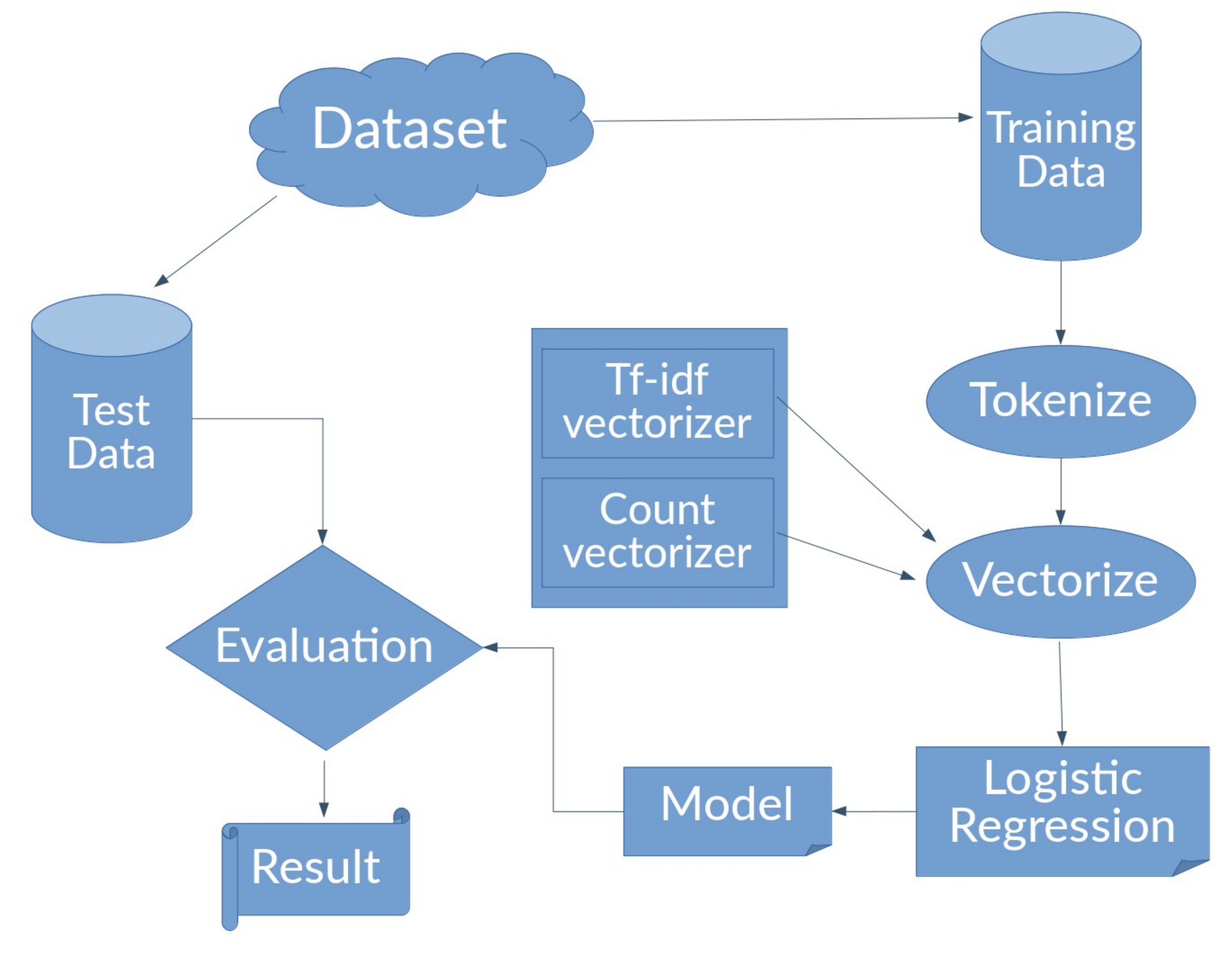
Maintenance best practices

Malicious URL detection tool (1 of 2)

Features of the tool:

- High portability towards operating sytem
- Use of Logistic Regression on Malicious URL dataset
- Choice of vectorizer: **count** and **tf-idf**
- Easy implementation of Chrome and Firefox extension
- Design diagram (.....Continued)

Malicious URL detection tool (2 of 2)



Results

- Malicious URL detection tool:
  - For count vectorizer
    - Accuracy rate of **99.3%**
  - For tf-idf vectorizer
    - Accuracy rate of **98.4%**
- Web Browser Security Assurance Maturity Model
  - Improvements over OWASP’s Software Assurance Maturity Model
  - Improvements over SEI’s Capability Maturity Model

References

- M. Vervier, M. Orrù, B. J. Wever, E. Sesterhenn, *“Browser Security White Paper',’* X41 D-SEC GmbH, Dennewartstr. 25-27 D-52068 Aachen Amtsgericht Aachen: HRB19989, September 2017.
- I. M. Heiderich, A. Inführ, F. Fabler, N. Krein, M. Kinugawa, T. C. Hong, D.Weiber, P. Pustulka, *“Cure53 Browser Security White Paper,”* Bielefelder Str. 14, D 10709, Berlin, cure53.de, November 2017.
- W. Alcorn, C. Frichot, M. Orrù, *“The Browser Hacker’s Handbook”*, Wiley publishing, USA, ISBN: 978-1-118-66209-0 ISBN: 978-1-118-66210-6 (ebk), 2014
- Patil Shital Satish, Chavan R. K, *Web Browser Security: Different Attacks Detection and Prevention Techniques.* International Journal of Computer Applications (0975 – 8887) Volume 170 – No.9, July 2017
- J. Grossman, R. Hansen, P. D. Petkov, A. Rager, S. Fogie, *“XSS Attacks: Cross Site Scripting Exploits and Defense,”* Syngress publishing, USA, 2007, ISBN- 13: 978-1-59749-154-9.
- Malicious URL dataset, KDNuggets.com

Thank you.