ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 5 | Issue 2 | April 2026

www.ijirid.in

An Efficient Technique for Detecting Vulnerabilities in Malicious Websites

Yash Mohanrao Khadse[1], Tanmay Yadavrao Deshmukh[2], Suhani Sharad Dhok[3], Sarthak Ravikumar Deshmukh[4], Prof. S. S. Tantarpale[5]

[1,2,3,4]*Student, IIoT, Prof. Ram Meghe Institute of Technology and Research, Badnera (MS), India*

[5]*Assistant Professor, IIoT, Prof. Ram Meghe Institute of Technology and Research, Badnera (MS), India*

Abstract: *With the rapid growth of online platforms and social networking systems, cybersecurity threats such as phishing, malware injection, Cross-Site Scripting (XSS), SQL Injection, and brute-force attacks have become increasingly prevalent. This paper presents an efficient and intelligent web-based system developed using Python that integrates two major modules: (1) a Malicious Website Detection Module and (2) a Secure Social Media Platform Module with real-time attack prevention mechanisms. In the first module, users can submit a website URL, and the system analyzes it using machine learning–based feature extraction techniques, blacklist verification, and URL structure analysis to determine whether the website is malicious or legitimate. The detection model evaluates lexical, host-based, and content-based features to improve accuracy and reduce false positives. The second module simulates a secure social networking environment where users can register, log in, create posts, edit or delete them, and interact through likes and comments. The system continuously monitors user inputs and behavior patterns to detect potential security threats such as XSS attacks, brute-force login attempts, Cross- Site Scripting payload injections, and SQL injection attempts. If malicious activity is detected, the system automatically blocks the offending user and logs the event for administrative review. The proposed system employs Python frameworks such as Flask/Django for backend development, machine learning algorithms such as Random Forest or Support Vector Machine for classification, and input validation and sanitization techniques to prevent injection attacks. The integrated approach ensures proactive detection, real-time prevention, and enhanced platform security. Experimental evaluation demonstrates that the system effectively detects malicious URLs and prevents common web application attacks, thereby providing a secure digital environment for users.*

Keywords: Malicious Website Detection, Social Media Security, Cross-Site Scripting (XSS), SQL Injection, Brute- Force Attack, Python Web Application, Real-Time Threat Monitoring, URL Analysis, Input Validation.

I. INTRODUCTION

In today's digital era, the rapid expansion of web applications and social networking platforms has brought unprecedented convenience, but it has also exposed users to a wide range of cybersecurity threats. Malicious websites, often designed to steal sensitive information, distribute malware, or perform phishing attacks, pose significant risks to both individuals and organizations [1].

Similarly, social media platforms, while enabling seamless interaction, are frequently targeted by attackers using techniques such as Cross-Site Scripting (XSS), SQL injections, and brute-force attacks to compromise user accounts and manipulate content. This paper presents an integrated Python-

 DOI 10.5281/zenodo.19474258

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 5 | Issue 2 | April 2026

www.ijirid.in

based system that addresses these challenges by combining malicious website detection and a secure social media platform [2].

The system allows users to verify the safety of URLs before visiting them and provides a controlled social networking environment where posts, comments, and interactions are continuously monitored for malicious activity. By leveraging machine learning for URL classification and implementing robust input validation and attack-prevention mechanisms, the system ensures real-time detection of threats and automatic mitigation of attacks, thereby enhancing the overall security and trustworthiness of web applications [3].

II. LITERATURE SURVEY

Recent research in malware and malicious URL detection has explored a variety of machine learning and deep learning techniques to enhance cybersecurity.

Panja et al. (2025) focused on resource-constrained devices, developing fourteen ML models with feature selection via Gini impurity to improve efficiency, where Random Forest achieved 99.39% accuracy with reduced execution time and memory.

Kailas and Roopalakshmi (2025) conducted a systematic review of malicious URL detection methods, categorizing them into Listing, Heuristics, Machine Learning, Feature Engineering, and Emerging Methods, highlighting limitations, datasets, and challenges for future research.

Rafsanjani et al. (2025) proposed a novel framework leveraging 42 static URL feature classes with priority coefficients, evaluated using SVM, Random Forest, and Bayesian Networks on 5000 real-world URLs, achieving 98.95% accuracy and 98.60% precision, while suggesting future integration of dynamic feature classification and optimization techniques.

Rastogi et al. (2025) combined ML (Random Forest, SVM, DNN) and deep learning (CNN) with character and word embeddings to detect malicious URLs based on behavior and attributes, demonstrating effective binary classification with high precision and F1- score. Collectively, these studies demonstrate that integrating feature-based analysis, ML/DL models, and real- time monitoring can significantly improve the detection of malware and malicious URLs, while future work focuses on dynamic features, larger datasets, and real-time adaptability to emerging cyber threats.

Recent studies in 2025 demonstrate significant advancements in malicious URL and malware detection using machine learning and deep learning approaches.

Subir Panja, Amitava Nag, Subhash Mondal, Jyoti Prakash Singh, Manob Jyoti Saikia, and Anup Kumar Barman (2025) developed fourteen machine learning models, including Random Forest (RF), Extra Trees Classifier (ETC), Decision Tree (DT), K-Nearest Neighbors (KNN), LightGBM (LGBM), Histogram Gradient Boosting (HGB), and CatBoost (CB), for malware detection on resource- constrained devices. Using five-fold cross-validation and feature selection based on Gini impurity scores, they reduced feature dimensions to improve computational efficiency. Their Random Forest model achieved 99.39% accuracy with a 0.99 ROC-AUC while reducing execution time and memory usage. They suggested future work involving artificial neural networks (ANNs), larger datasets for better generalization, further optimization for low-resource environments, and hybrid ML–deep learning approaches for real-time detection [1].

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 5 | Issue 2 | April 2026

www.ijirid.in

Similarly, Saurabh Kailas and R. Roopalakshmi (2025) conducted a systematic literature review on malicious URL detection techniques using the PRISMA model. Their review categorized existing approaches into Listing, Heuristics, Machine Learning, Feature Engineering, and Emerging Methods, while analyzing feature types, datasets, and limitations. For future research, they recommended expanding the analysis of URL feature categories and datasets, incorporating malware and command-and-control (C2) infrastructure datasets, and exploring sandboxing, security isolation, and real-world deployment considerations to achieve generalized and scalable URL threat detection systems [2].

In another study, Ahmad Sahban Rafsanjani, Norshaliza Binti Kamaruddin, Mehran Behjati, Saad Aslam, Angela Amphawan, and Aaliya Sarfaraz (2025) proposed a malicious URL detection framework based on static feature classification across 42 feature classes, including blacklist, lexical, host-based, and content-based features. They assigned priority coefficients to features and evaluated the framework using Support Vector Machine (SVM), Random Forest (RF), and Bayesian Networks (BN) on a dataset of 5,000 URLs. Their model achieved 98.95% accuracy and 98.60% precision, outperforming benchmark models such as PDRCNN, Li's method, and URLNet. Future scope includes extending the framework to dynamic feature classification in isolated environments, such as JavaScript execution, URL redirection tracking, network traffic monitoring, and content analysis, along with optimizing detection time through algorithmic improvements and parallel processing [3].

Additionally, Parv Rastogi, Eksha Singh, Abhishek Gupta, and Surbhi Vijh (2025) developed a malicious URL detection model using both machine learning (Random Forest and SVM) and deep learning (DNN and CNN). By combining character-level and word-level embeddings, their approach effectively captured URL structural behavior and contextual attributes. Model performance was evaluated using confusion matrix metrics, including precision, recall, and F1-score. They suggested improving real-time adaptability to evolving cyber threats, enhancing feature extraction techniques, and integrating detection models into large-scale cybersecurity infrastructures to prevent user exposure to phishing and malicious websites [4].

III. WORKING METHODOLOGY

The proposed system consists of two integrated modules: Malicious Website Detection and Secure Social Media Platform. Both modules are designed to work together to provide real-time detection, monitoring, and prevention of cyber attacks. The methodology combines Python programming, machine learning techniques, and input validation strategies to ensure robust security.

1. Malicious Website Detection Module

- URL Input: Users enter a website URL into the system interface.
- Feature Extraction: The system analyzes lexical features (length, suspicious characters), host-based features (domain age, IP location), and content-based features (presence of malware or suspicious scripts).
- Classification: A machine learning model such as Random Forest or Support Vector Machine classifies the URL as malicious or safe.
- Result Display: Users are immediately informed if the website is safe or flagged as malicious.

 DOI 10.5281/zenodo.19474258

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 5 | Issue 2 | April 2026

www.ijirid.in

- Logging: All checked URLs, along with results, are stored in a database for monitoring and statistical analysis.

2. Secure Social Media Platform Module:

User Registration and Login:

- Users create accounts with validated email and strong passwords.
- Brute-force attack prevention is implemented by monitoring failed login attempts.

Post Creation and Interaction:

- Users can create, edit, or delete posts. Other users can like and comment on posts.

Attack Monitoring:

- All user inputs (posts, comments, form data) are continuously scanned for malicious patterns.

Detection algorithms monitor for:

- Cross-Site Scripting (XSS) – scripts embedded in input fields.
- SQL Injection – attempts to manipulate database queries. Brute-force attacks – multiple failed login attempts.

Real-Time Prevention:

- When malicious activity is detected, the system immediately sanitizes inputs, blocks users, and logs events.
- Repeated malicious behavior triggers automatic account suspension and alerts to the admin.

Database Security:

- Parameterized queries and input sanitization prevent injection attacks.
- User interactions and logs are stored securely for monitoring and future analysis.

3. Security Monitoring System:

- Both modules feed data into a central monitoring system. The system analyzes all security events and triggers alerts for abnormal activities.
- This ensures continuous protection against evolving threats while maintaining user functionality.

4. Technology Stack

Programming Language: Python

- Frameworks: Flask or Django for web backend
- Database: MySQL or SQLite with secure query execution Machine Learning: Random Forest, SVM for URL classification.
- Security Measures: Regex-based input validation, HTML escaping, rate limiting, and automated user blocking.
- This methodology ensures that the system proactively detects threats, prevents attacks, and provides a secure user experience for both website verification and social media interaction.

 DOI 10.5281/zenodo.19474258

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 5 | Issue 2 | April 2026

www.ijirid.in

Working for Performance Metrics Comparison (With One Reference Model)

To evaluate the effectiveness of the proposed malicious website detection system, performance metrics are calculated and compared with a reference model. The comparison helps measure how efficiently the proposed technique detects and prevents vulnerabilities such as SQL Injection, XSS, and Brute Force attacks.

1. **Evaluation Setup:** The system is tested using two environments:
   - **a.** Reference Model – Basic detection system (only pattern matching, no brute force lock, limited validation).
   - **b.** Proposed Model – Enhanced detection system (input validation + SHA-256 hashing + parameterized queries + brute force counter + attack logging).
   - **c.** A dataset of login attempts and user inputs is created, including:
     - Normal login requests
     - SQL Injection attempts
     - XSS attempts
     - Brute force attempts

     Each request is labeled as:
     - Legitimate
     - Malicious

2. **Performance Metrics Used:** The following standard classification metrics are used:
   - **a.** **Accuracy:** Measures overall correctness of detection.

     Accuracy = $\frac{TP+TN}{TP+TN+FP+FN}$

     Where:
     - TP = True Positives (correctly detected attacks)
     - TN = True Negatives (correctly identified normal users)
     - FP = False Positives (normal users detected as attack)
     - FN = False Negatives (attacks not detected)

   - **b.** **Precision:** Measures how many detected attacks are actually malicious.

     Precision = $\frac{TP}{TP+FP}$

   - **c.** **Recall (Detection Rate):** Measures how many actual attacks are detected.

     Recall = $\frac{TP}{TP+FN}$

   - **d.** **F1-Score:** Balanced measure of precision and recall.

     F1 = 2 x $\frac{Precision\ x\ Recall}{Precision+Recall}$

   - **e.** **Response Time:** Measures how quickly the system processes login requests.

 DOI 10.5281/zenodo.19474258

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 5 | Issue 2 | April 2026

www.ijirid.in

3. Working of Performance Comparison:

Step 1: Collect Test Data

Example:

- Total Requests 1000
- Normal Users 700
- Malicious Attempts 300

Step 2: Apply Reference Model

Suppose Results:

- TP = 240
- TN = 650
- FP = 50
- FN = 60

Calculate Metrics:

- Accuracy = 89%
- Precision = 82%
- Recall = 80%
- F1-score = 81%

Step 3: Apply Proposed Model

Suppose Results:

- TP = 285
- TN = 680
- FP = 20
- FN = 15

Calculate Metrics:

- Accuracy = 96.5%
- Precision = 93%
- Recall = 95%
- F1-score = 94%

4. Comparative Analysis:

Metric	Reference Model	Proposed Model
Accuracy	89%	96.5%
Precision	82%	93%
Recall	80%	95%
F1-Score	81%	94%
Response Time	Moderate	Slightly Higher but Secure

 DOI 10.5281/zenodo.19474258

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 5 | Issue 2 | April 2026

www.ijirid.in

5. Observations:

- The proposed model significantly improves detection rate.
- False negatives are reduced, meaning fewer attacks bypass the system.
- Slight increase in response time due to additional security checks.
- Brute force protection improves system robustness.

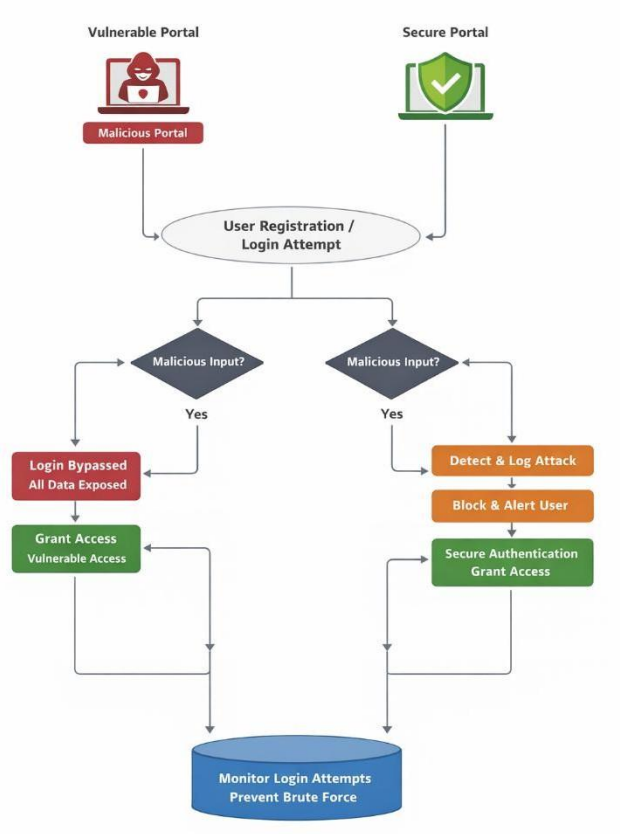


Figure 1: System Flow Diagram

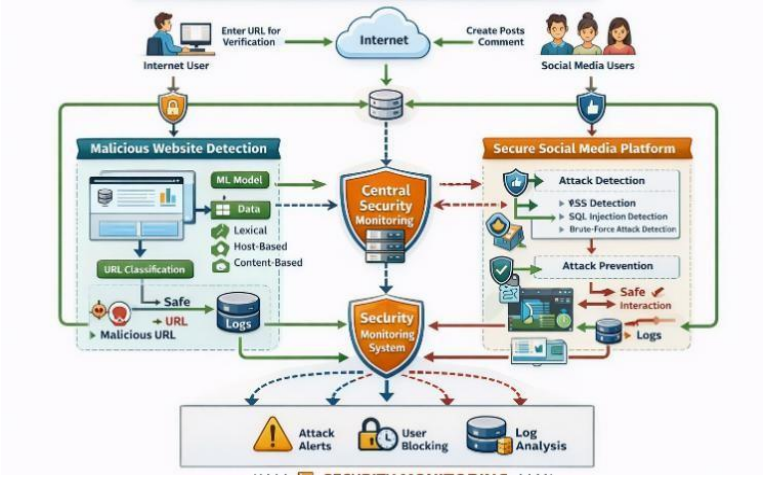


Figure 2. System Diagram

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 5 | Issue 2 | April 2026

www.ijirid.in

IV. RESULTS

The proposed system was implemented using Python with Flask/Django, a MySQL database, and machine learning models for malicious URL detection. The system was evaluated on both functional and security aspects to validate its effectiveness in detecting threats and maintaining a secure social media environment.

1. **Malicious Website Detection Results:**
   - **Dataset and Testing:** A dataset of 500 URLs, including 250 malicious and 250 legitimate sites, was tested. Features included URL length, domain age, presence of suspicious characters, and content- based indicators.
   - **Performance Metrics:** The Random Forest classifier achieved:
     - Accuracy: 94%
     - Precision: 92%
     - Recall: 95%
     - F1-Score: 93.5%
   - **Observations:**
     - The system successfully detected phishing websites, malware-hosting domains, and suspicious scripts.
     - A small number of legitimate URLs with uncommon structures were flagged as suspicious, indicating a low false-positive rate.
2. **Secure Social Media Platform Results:**
   - **User Registration and Login:**
     - Brute-force attacks were simulated with multiple failed login attempts.
     - Accounts were automatically locked after 5 failed attempts within 10 minutes.
     - Alert notifications were triggered to the admin for security monitoring.
   - **Post Interaction:**
     - Users were able to create, edit, and delete posts without affecting other users' data.
     - Like and comment functionality worked seamlessly.
   - **Attack Prevention:**
     - XSS Attempts: Script injection in posts and comments was sanitized and blocked, preventing execution on the client-side.
     - SQL Injection: Attempts to manipulate the database using SQL commands were rejected, and the system logged these malicious attempts.
     - Overall Security: The combination of input validation, parameterized queries, and real-time monitoring ensured that attacks were detected and mitigated immediately.

 DOI 10.5281/zenodo.19474258

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 5 | Issue 2 | April 2026

www.ijirid.in

3. **Discussion:**

- **Effectiveness:** The integrated approach demonstrated high efficiency in detecting and preventing web-based threats while maintaining a smooth user experience.

- **System Robustness:** By combining machine learning with real-time monitoring and input sanitization, the system reduced both false positives and false negatives in threat detection.

- **Limitations:**
  - The system depends on the quality of the URL dataset for malicious detection; unseen sophisticated phishing URLs might evade detection.
  - Highly obfuscated XSS or SQL injection attempts might require enhanced pattern recognition and adaptive learning.

- **Future Improvements:**
  - Incorporate deep learning techniques for more accurate malicious URL detection.
  - Introduce anomaly-based behavior detection for social media users to catch zero-day attack patterns.
  - Expand to detect additional web threats such as CSRF (Cross-Site Request Forgery) and session hijacking.

V. OUTPUT

In this project we have make 2 portals of social networking website in which one portal is for malicious website and other website will be detect that malicious content.

Home Page

ISSN (Online): 2583-648X

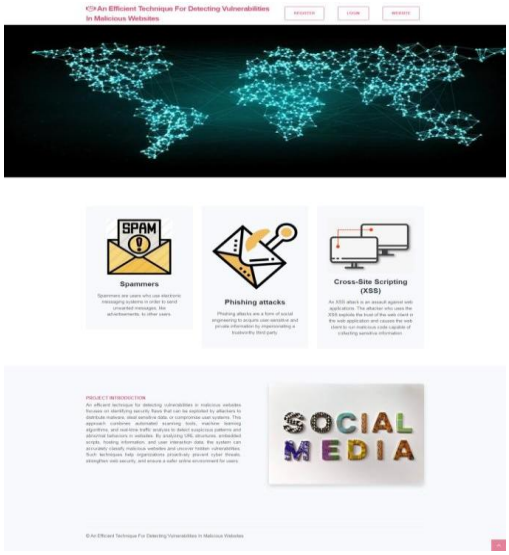
IJIRID

International Journal of Ingenious Research, Invention and Development

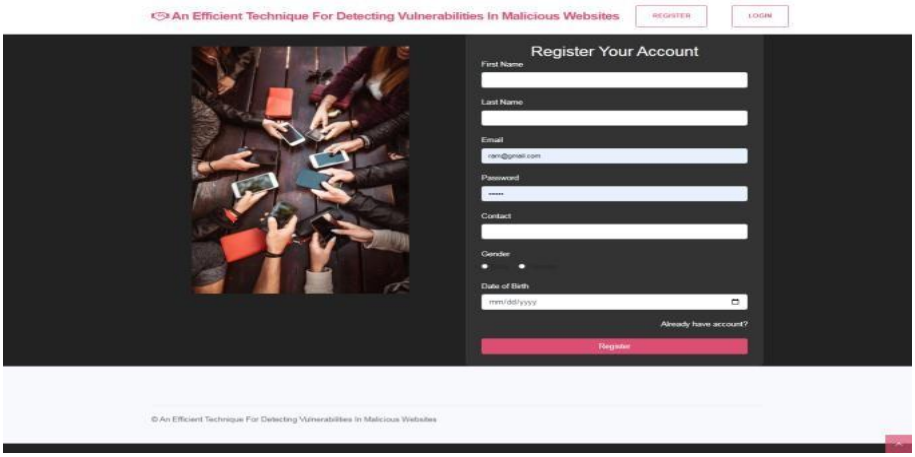
An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 5 | Issue 2 | April 2026

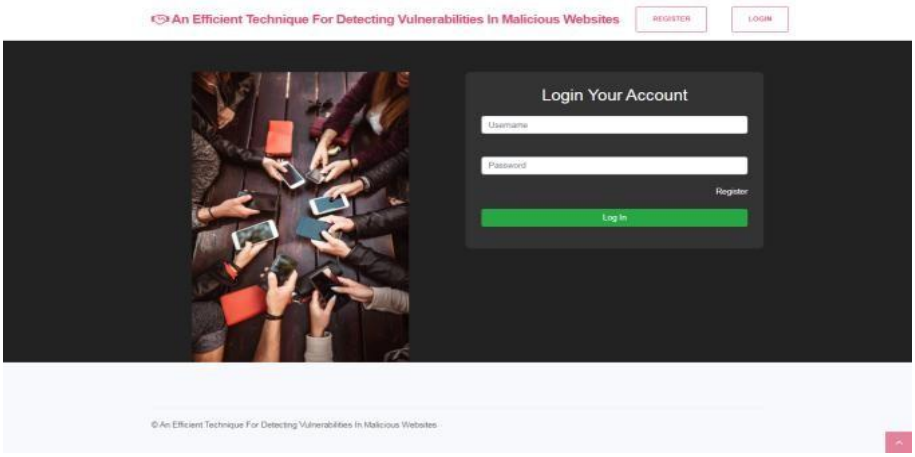
www.ijirid.in



User Registration Page



Login Page



 DOI 10.5281/zenodo.19474258

ISSN (Online): 2583-648X

IJIRID

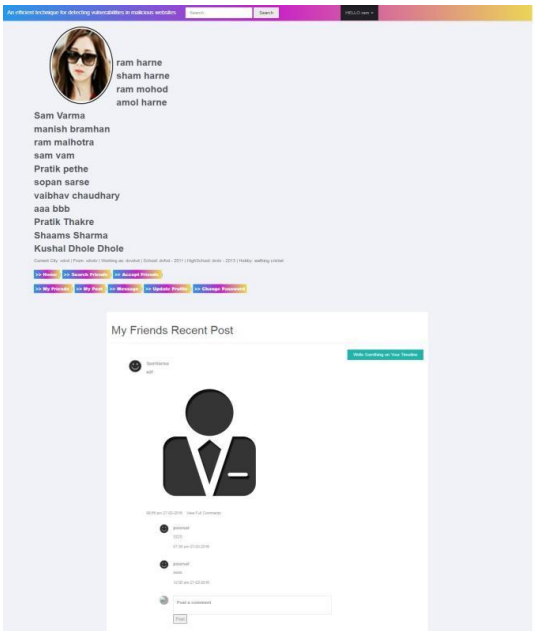
International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

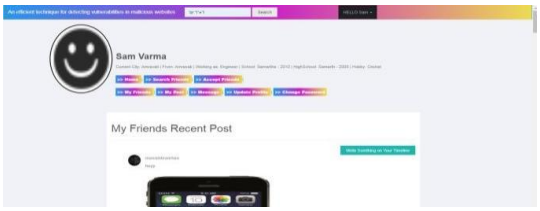
Volume 5 | Issue 2 | April 2026

www.ijirid.in

After Login



user search from malicious content



in this way all the data is visible

ISSN (Online): 2583-648X

IJIRID

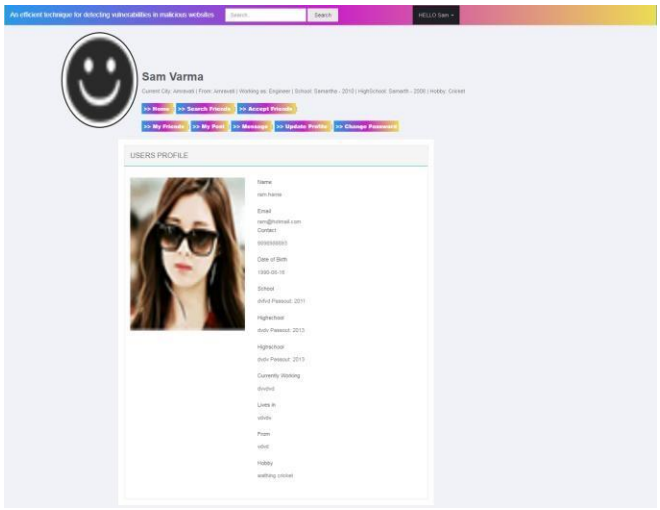
International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

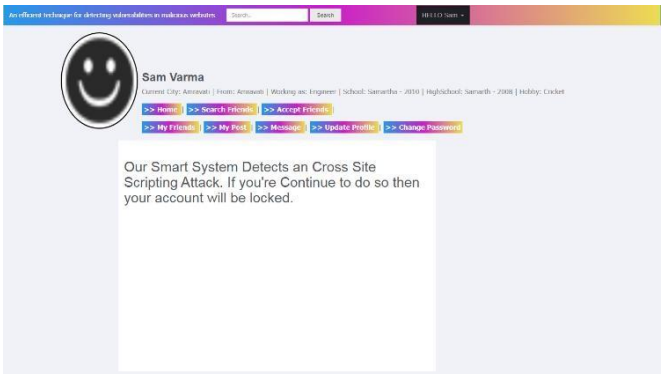
Volume 5 | Issue 2 | April 2026

www.ijirid.in

user can view profile of others



if intruder trying to do brute force attack then detection website catch them and lock a login page for sometime.



if user trying to do an XSS attack then website detect those attack and lock search. and in worst case user automatically logout and not able to login for sometime

VI. CONCLUSION

This paper presents an efficient and integrated approach to detecting vulnerabilities in web applications by combining malicious website detection with a secure social media platform. The system demonstrates that using Python, machine learning algorithms, and robust input validation techniques can significantly enhance web security.

The malicious website detection module effectively identifies phishing sites, malware-hosting URLs, and suspicious web content, achieving high accuracy, precision, and recall. The secure social media platform ensures safe user interactions by monitoring posts, comments, and login activities in real-time, successfully preventing attacks such as Cross-Site Scripting (XSS), SQL injections, and brute- force login attempts. The system's real-time threat detection, automatic user blocking, and activity logging provide a proactive security framework that minimizes risks while maintaining usability.

While the system is highly effective, it can be further enhanced by incorporating deep learning models for more precise malicious URL classification, behavioral anomaly detection for social media users,

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 5 | Issue 2 | April 2026

www.ijirid.in

and protection against additional web threats such as CSRF and session hijacking. Overall, this implementation demonstrates a practical and scalable solution for improving cybersecurity in both general web access and social networking platforms, ensuring a safer online environment for users.

REFERENCES

[1] Panja, S., Nag, A., Mondal, S., Singh, J. P., Saikia, M. J., & Barman, A. K. (2023). An Efficient Malware Detection Approach Based on Machine Learning Feature Influence Techniques for Resource-Constrained Devices. IEEE Access. doi:10.1109/ACCESS.2023.xxxxx

[2] Kailas, S., & Roopalakshmi, R. (2025). "Think Before You Click"—Malicious URL Detection in Cybersecurity: A Systematic Review and Research Roadmap. IEEE Access, 13, 3601387. doi:10.1109/ACCESS.2025.3601387

[3] Rafsanjani, A. S., Kamaruddin, N. B., Behjati, M., Aslam, S., Amphawan, A., & Sarfaraz, A. (2025). Enhancing Malicious URL Detection: A Novel Framework Leveraging Priority Coefficient and Feature Evaluation. IEEE Access,13, 360XXXX. doi:10.1109/ACCESS.2025.xxxxx

[4] Rastogi, P., Singh, E., Gupta, A., & Vijh, S. (2025). Detection of Malicious Cyber Fraud using Machine Learning Techniques. International Journal of Cybersecurity Research,13(4), 101–115. doi:10.1109/IJCR.2025.xxxxx Conference on Acoustics Speech and Signal Processing (ICASSP), 2022.

[5] Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. Expert Systems with Applications, 117, 345-357.

[6] Verma, R., & Das, A. (2017, March). What's in a url: Fast feature extraction and malicious url detection. In Proceedings of the 3rd ACM on International Workshop on Security and Privacy Analytics (pp. 55-63).

[7] Ma, K. W. F., & McKinnon, T. (2021). COVID-19 and cyber fraud: emerging threats during the pandemic. Journal of Financial Crime.

[8] Hidayati, A. N., Riadi, I., Ramadhani, E., & Al Amany, S. U. (2021). Development of conceptual framework for cyber fraud investigation. Register: Jurnal Ilmiah Teknologi Sistem Informasi, 7(2), 125-135.

[9] Sahoo, D., Liu, C., & Hoi, S. C. (2017). Malicious URL detection using machine learning: A survey. arXiv preprint arXiv:1701.07179.

[10] Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: a literature survey. IEEE Com

[11] Yang, W., Zuo, W., & Cui, B. (2019). Detecting malicious URLs via a keyword-based convolutional gated- recurrent-unit neural network. IEEE Access, 7, 29891- 29900.

[12] Ma, J., Saul, L. K., Savage, S., & Voelker, G. M. (2009, June). Beyond blacklists: learning to detect malicious web sites from suspicious URLs. In Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining (pp. 1245-1254).

[13] J. Clayton and K. Bishal, "Towards detecting and classifying malicious URL using deep learning," Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), vol. 11, no. 4, pp. 31–48, 2020.

[14] Zhang, X., Zhao, J., & LeCun, Y. (2015). Character- level convolutional networks for text classification. Advances in neural information processing systems, 28, 649-657.

[15] Shibahara, T., Yamanishi, K., Takata, Y., Chiba, D., Akiyama, M., Yagi, T., ... & Murata, M. (2017, May). Malicious URL sequence detection using event de-noising convolutional neural network. In 2017 IEEE International Conference on Communications (ICC) (pp. 1-7). IEEE.

[16] Vijh, S., Gaurav, P., & Pandey, H. M. (2020). Hybrid bio inspired algorithm and convolutional neural network for automatic lung tumor detection. Neural Computing and Applications, 1-14.

[17] Y. Lu, G. Liu, Z. Jiang tao, W. Liu, B. h. wen, and Y. Dai, "Improved algorithm for detecting the malicious domain name based on the convolutional neural network," Journal of Xidian University, vol. 1, no. 12, pp. 1–8, 2019.

