

OSINT-BOT Risk Assessment Matrix					
Risk	Description	Likelihood	Impact	Mitigation	Responsibility
Leaked Metadata from Web Scraping	Inadvertent exposure or leakage of sensitive metadata (such as IP addresses, user-agent details, or request timing) that could be traced back to the user or organization.	Medium	High	Use proxies and rotate them regularly to mask real IP addresses. Implement rate limiting to mimic human browsing patterns and avoid detection. Ensure adherence to website terms of service and legal requirements regarding data scraping.	IT Security Team
Malicious Use of the Software	Misuse of the software to perform unauthorized or illegal web scraping, potentially leading to legal repercussions and reputational damage.	Low	Very High	Implement logging features to track usage patterns and detect unusual activities. Require user authentication and define strict usage policies. Provide training on ethical and legal standards related to web scraping.	Compliance Officer
System Performance Degradation	The software could significantly slow down the system performance, affecting other operations due to high CPU or memory usage during intensive scraping tasks.	Medium	Medium	Optimize code to be more efficient. Implement system resource checks to ensure the software does not exceed predefined resource limits. Use asynchronous programming to handle long-running tasks.	Development Team
Data Integrity Issues	Incorrect or incomplete data capture during web scraping which could lead to faulty analytics or decisions based on the scraped data.	High	High	Implement checks to validate and sanitize incoming data. Use redundant scraping methods to verify and cross-check data. Regularly update scraping algorithms to adapt to changes in source website structures.	Quality Assurance Team