Ethical Hacking Technical Report

Client: www.y8.com

Date: May 18, 2024

Prepared by: Hadjie Alayan and Luigi Alayan

Executive Summary: This report presents the technical findings of the ethical hacking assessment conducted for www.y8.com. The assessment aimed to identify vulnerabilities within the organization's network infrastructure, applications, and systems. Through various testing methodologies, including penetration testing and vulnerability scanning, critical and high-risk issues were discovered.
This report provides detailed descriptions of these findings, along with actionable recommendations for remediation.

Vulnerability Summary:

1. Outdated Software Components: The website utilizes outdated software components, exposing it to known vulnerabilities.
2. Insecure File Uploads: The website allows users to upload files without proper validation, potentially leading to the execution of malicious code.
3. SQL Injection: The website is vulnerable to SQL injection attacks, enabling attackers to manipulate databases and access sensitive information.
4. Missing Security Headers: HTTP security headers such as Content Security Policy (CSP) and X-Frame-Options are not properly configured, leaving the website vulnerable to various attacks.
5. Weak Password Policies: Users are allowed to set weak passwords, increasing the risk of unauthorized access through brute force attacks.
6. Lack of Input Validation: Input fields on the website lack proper validation, making it vulnerable to injection attacks.
7. Exposed Directory Listings: Directory listings are exposed, potentially revealing sensitive information about the website's directory structure.
8. Insecure Third-Party Integrations: Third-party integrations used on the website have known vulnerabilities that could be exploited by attackers.
9. Missing Security Updates: Critical security updates for server software are not applied promptly, exposing the website to exploitation.
10. Insecure Session Management: Session tokens are not properly managed, leaving the website vulnerable to session hijacking attacks.
11. Sensitive Information Disclosure: Error messages reveal sensitive information about the website's underlying technology stack, aiding attackers in reconnaissance.
12. Inadequate Access Controls: Certain pages or functionalities on the website lack proper access controls, allowing unauthorized access to sensitive information.
13. Open Redirects: The website contains open redirect vulnerabilities that could be exploited by attackers to redirect users to malicious websites.

Recommendations:

1. Update Software Components: Ensure all software components are up to date to patch known vulnerabilities.
2. Validate File Uploads: Implement file type verification and malware scanning to prevent the upload of malicious files.
3. Secure Third-Party Integrations: Regularly update and monitor third-party integrations for security patches and vulnerabilities.
4. Enforce Strong Password Policies: Enforce password complexity requirements and implement account lockout mechanisms to deter brute force attacks.
5. Disable Directory Listings: Disable directory listings to prevent exposure of sensitive information.
6. Apply Security Updates Promptly: Regularly apply security updates for server software to mitigate known vulnerabilities.
7. Implement Secure Session Management: Use secure cookies and session tokens to prevent session hijacking attacks.
8. Minimize Error Information: Customize error messages to avoid disclosing sensitive information about the website's infrastructure.
9. Implement Access Controls: Implement proper access controls to restrict access to sensitive pages and functionalities.

Conclusion:

Addressing the identified vulnerabilities and implementing the recommended remediation measures is crucial to enhance the security posture of the website. Continuous monitoring and regular security assessments are recommended to ensure ongoing protection against emerging threats.