

Web Security Analysis chest Sibolga City District Court Class 2a with Penetration Testing

Rion Dui Haryadi Samosir¹, Akhyar Lubis², Supina Batubara³


^{1,2}Department of Computer Engineering, Universitas Pembangunan Panca Budi, Indonesia

³Department of Computer System, Universitas Pembangunan Panca Budi, Indonesia

ABSTRACT

Web security analysis is a very important thing to do, especially for organizations or agencies that depend on web technology in carrying out their business activities and managing data and information. The popularity of web-based applications makes the web itself vulnerable to security threats, such as cyberattacks, which can have an impact on data integrity and confidentiality. One of the web security assessment analyses can be done by penetration testing. Web security assessment testing needs to be done to identify vulnerabilities then if the vulnerability is determined it will be easier to develop an effective mitigation strategy. This research will conduct experiments with penetration testing methods by simulating web attacks with OWASP top 10. The results of the research will be recommendations given including the implementation of security configurations more optimally, CMS updates, strict access control settings, and increased security awareness for users who are directly connected to website-based applications. Configuration errors can also result in valuable information being extracted from the system. Conducting regular web security analysis, organizations or agencies using web-based applications can identify and overcome vulnerabilities before they are exploited by irresponsible parties. This enables organizations to maintain the security and integrity of web systems, as well as protect critical digital assets, especially valuable data.

Keyword : Analysis; Web; Penetration Testing

 This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Corresponding Author:

Akhyar Lubis,
Department of Computer Engineering
Universitas Pembangunan Panca Budi
Jl. Jend. Gatot Subroto Km. 4,5 Sei Sikambang Medan, Indonesia.
Email : akhyarlbs@dosen.pancabudi.ac.id

Article history:

Received May 20, 2024
Accepted May 26, 2024

1. INTRODUCTION

The use of information technology today such as double-edged knives, can be positive values such as profitability, efficiency, data security, more savings, and minimizing human resources involved [1], [2], [3]. But behind all the advantages there is also a negative side caused, namely valuable data connected to the internet can also be stolen or experience other cybercrimes [4]. Every organization or government or private agency must be able to secure data from the threat of data leakage attacks[5] [6]. Computer crime is varied and very diverse [7], But the biggest problem is from outside parties[8]. Sibolga City District Court Class 2A utilizes web technology to manage information and services, The application used is web-based accessed by users with an internet connection or intranet [9], [10], [11]. However, the web is vulnerable to security threats, such as cyberattacks, which can impact data integrity and confidentiality. Based on article 15 of the ITE Law, it requires that every electronic system operator is safe, reliable and responsible and can operate as it should. There is a word physically and nonphysically safe. Therefore, web security analysis with penetration testing needs to be done to identify vulnerabilities.

Bank Indonesia regulation on the implementation of risk management in the use of information technology by commercial banks states that penetration testing of internal networks and external networks must be carried out at least once a year. So, it is necessary to identify security weaknesses both in terms of applications, computers and networks. So that there is a security evaluation so that it can correct the weaknesses of the system that are found before being used for crime. Controlling vulnerabilities and threats can minimize the risks posed. The method used uses vulnerability assessment

and penetration tests. This research will focus on web applications that run on the web server of the Sibolga City District Court. Web security analysis is done by penetration testing with OWASP incorporation. This study aims to find weaknesses or vulnerabilities that exist in the Sibolga City District Court web application as an information center by conducting an existing security evaluation. The method used with attack simulation so that security holes are known in web-based applications with OWASP and EC-Council models.

2. RESEARCH METHOD

In the initial stage, problem identification is carried out, then problem analysis is carried out and collecting research supporting theories. Previous research searches using Google Scholar with the aim of strengthening problems and becoming the basis for the method approach used in research. So the approach method with OWASP top 20 is used as a reference to the security risks of web applications and possible vulnerabilities that will arise [12], [13], [14]. Then target setting and data collection [12], [13], [14], [15], [16], [17], [18], [19], [20]. Data collection is done to collect information related to web applications that are set as targets of penetration testing nature. Data collection is carried out as much as possible against the targets that have been set. This is the beginning of preparation in the penetration testing process. The technique is carried out by scanning internal tissue and scanning external tissue. OWASP top 10 uses a summary of 10 security holes in malicious applications so that they become the basis for carrying out the next steps and steps. This study uses Tools, Nmap, xprobes2 in obtaining information by scanning ports, operating systems and service enumeration. Data collected network used, IP addressing used, operating system used, analyzing open ports used in scanning and vulnerability assessment.



Fig 1. Metode Penelitian

A. Workflow

Prose research uses a web-based application penetration testing method approach in analyzing web security by identifying, analyzing and reporting vulnerabilities such as:

1. Input validation, to identify vulnerabilities related to insufficient input validation in web applications by testing with special character inputs, malicious scripts, or invalid inputs in input fields in web applications.
2. Buffer overflow, to identify vulnerabilities related to buffer overflow in web applications. Enter inputs that exceed the storage limit in the web application input field.
3. Sql injection, to identify vulnerabilities related to SQL Injection in web applications, using special characters or SQL queries in web application input fields.
4. Bypassing authentication, Identifies authentication-related vulnerabilities in web applications. by exploiting loopholes, such as using default credentials, brute-force, or exploiting weaknesses in authentication mechanisms.
5. Code Excretion, to identify vulnerabilities related to code execution in web applications. with malicious code or script input on the input field of the web application.

The above Work Process can run smoothly with the minimum specifications of supporting equipment as follows:

1. One unit of Lenovo core i5 laptop with 8GB RAM with 1 TB hard drive capacity.
2. Wireless adapter leguang N960, chipset relink RT3070, 802,11bgn.
3. Windows 10 preinstalled linux with virtualization.

B. Analysis Methods

Web application security analysis:

1. Input Validation:
 - OS Command Injection: Attempts to enter malicious operating system commands in the input field to see if the application is vulnerable to command injection.
 - Script Injection: Inserts malicious scripts (such as JavaScript) in input fields to test whether an application can be infected by cross-site scripting (XSS).
 - SQL Injection: Attempts to insert malicious SQL queries on input fields to identify SQL injection vulnerabilities.
 - LDAP Injection: Inserts malicious strings in input fields associated with LDAP to check for LDAP injection vulnerabilities.
 - Cross-Site Scripting (XSS): Tests whether an application can be exploited by inserting a malicious script in the input field.
2. Output sanitization, its function of checking the web application adequately sanitizes (cleans) the output displayed to users to prevent XSS attacks.
3. Checek for buffer overflows, test covers on attacks against stack overflow, heap overflow, format string overflow.
 - Stack Overflow, attempts to enter inputs that exceed the buffer limit on the application to check if there is a stack overflow vulnerability.
 - Heap Overflow: Tests whether an application is vulnerable to heap overflow by entering inputs that exceed the buffer limit.
 - Format String Overflow: Tests whether an application is susceptible to format string overflow by entering an invalid format string.
4. Access Control, by testing authorization mechanisms and access rights management on applications to ensure that users can only access resources that match their level of privacy. Trying to bypass access control with techniques such as privilege escalation
5. Denial of Service, testing the DoS condition of the application by sending excessive input or requests to see if the application can be subverted. Test application reliability in handling overload situations or DoS attacks.

3. RESULTS AND DISCUSSION

The use of tools in the network laboratory with network surveys scans with an internet connection. Information is collected with subdomains of web-based applications, open ports, ip addresses, dns, web application firewall detection, operating system and fingerprint.

A. Sub Domain

Identify the subdomains owned by the application:

1. Subdomains can hide additional applications or services that are not officially registered. When finding subdomains can help map the entire application infrastructure.
2. Check the security of subdomains, Subdomains can have different configurations or access controls than the primary domain. Subdomains security testing can uncover undetected security holes in the primary domain.
3. Detects takeover subdomain, Unused or properly configured subdomains can be taken over by attackers. Subdomain testing can identify possible takeover subdomains.
4. Looking for sensitive information, Subdomains may contain sensitive information or content that should not be publicly accessed. Checking subdomains can help find leaked confidential data.
5. Test attack scenarios, Subdomains can be used as entry or jump points to attack core applications. Subdomain testing can evaluate the risk and impact of attacks through subdomains.

B. OS and Service Fingerprint

1. Identify the operating system, Specifies the operating system used by the web application server. Results from the Information find vulnerabilities specific to a particular operating system.
2. Detecting the operating system version is done to determine the operating system version used. An outdated version of the operating system or a known vulnerability can be a security flaw.
3. Identify services and servers used, detect the type and version of web servers, application servers, databases, and other services used. This information can be used to find specific vulnerabilities in those components.
4. Collect additional information such as IP address, hostname, and network configuration. This data can help broaden understanding of application infrastructure.
5. Methods that can be used for fingerprinting are HTTP header analysis, server response, and application banners, port scanning to detect running services, use of tools such as Nmap, Unicornscan, Amap, and Telnet, Web application source code analysis.

Information obtained from fingerprinting can be used to identify specific vulnerabilities in the components used, plan more targeted attacks, prioritize the repair of discovered vulnerabilities, provide recommendations for updating or migrating used components.

C. Web Application Firewall Detection

Detection of the presence of Web Application Firewall on web applications aims to:

1. Identify the presence or absence of WAF, knowing whether the web application uses WAF to protect itself. This information is important for planning proper security testing.
2. Determine, the type of WAF used, identify the vendor, model, or type of WAF implemented. This knowledge helps understand the specific capabilities and weaknesses of the WAF.
3. Understand, the functionality of WAF, evaluate the features provided by WAF, such as attack detection, filtering, and logging. This information is useful for designing attacks that might be able to bypass or fool the WAF.
4. Detect weaknesses or bad configuration of WAF, identify security holes or improper configuration of WAF. This information can be used to find ways to bypass or exploit WAF weaknesses.

Several techniques can be used for WAF detection.

1. Analysis of HTTP headers and server response
2. Testing with WAF-specific attack scenarios
3. Identify patterns or anomalies in network traffic
4. Use of tools such as WafW00f, wafw00f, and Wapiti

D. Scanning and Vulnerability Assessment

There are two techniques used in scanning, namely manual and automatic. Manual techniques take more time in identifying vulnerabilities. Automatic scanning and vulnerability assessment with Nessus. Nessus for scanners to see the operating system used as well as assess the vulnerability of services running on the target host. The results of the scan are used for exploitation against the target host. Network scanning is done with three steps or active devices, Operating System, IP used. The open port or close port then gaps. The results are presented in the nessus report for each scanned host and then labeled critical, high, low and medium. The value of each column is obtained notifying the points found using nessus in each column.

E. Exploitation

Security analysis with web application security penetration, at the exploitation stage is very important after scanning and vulnerability assessment. Exploitation is the process of exploiting previously identified security holes.

The objectives of exploitation are:

1. Vulnerability Verification, ensuring that identified vulnerabilities can be exploited. Gather more detailed evidence about the impact and consequences of such vulnerabilities.
2. Increased Access Rights, trying to gain higher access or greater privileges on the system. As an illustration such as from ordinary user to admin, or from limited access to full access.
3. Collection of Additional Information, by exploiting loopholes to exfiltrate sensitive data, configuration, or other internal information. Obtain more information that can be used for further attacks.
4. Test Attack Scenarios, try various exploitation techniques to assess the defense capabilities of the system. Evaluate the impact and effectiveness of the attack that can be carried out.

F. Scanner INURL

An inurl scanner is a search operator that can be used in scanning tools to identify web pages that contain certain information in their URLs. It can be used to find web pages that may be vulnerable to attack.

Some examples of using the "inurl:" command in scanning include:

1. Search the admin page or login panel, to identify the admin page or login that may have vulnerabilities.
2. Look for unsafe directories, which are often used to store backup or temporary files that may contain sensitive information.
3. Search for configuration files, the configuration files can contain important information about the system, which can be exploited by attackers.
4. Analyze pages by looking for pages with unsafe parameters. Parameters in URLs that are not filtered properly can be vulnerable to attacks such as SQL Injection.

G. Brute Force

Brute Force technique is one method that is often used in security testing, especially to break into user credentials (usernames and passwords).

In a Brute Force attack, automated tools will try to enter possible username and password combinations, systematically and repeatedly, until they find a valid combination.

Some examples of using Brute Force in security testing include:

1. Cracking Password, experiment various combinations of commonly used usernames and passwords. By utilizing a dictionary of words, numbers, and special characters that are often used in passwords. You can also use Wordlist or Hybrid Wordlist techniques to increase effectiveness.
2. Account Enumeration, experiment possible username combinations, such as admin, root, guest, etc. Aim to identify valid accounts on the system.
3. Increased Access Rights, after obtaining valid credentials, try to upgrade access rights to administrator or higher access.

Some tools that are often used for Brute Force attacks, among others, Hydra, Medusa, THC HydraJohn the Ripper. Although Brute Force can be an effective technique, it should be noted that its use should be done carefully and within permissible restrictions. Too many access attempts in a short period of time can cause disruption to the target system and trigger security measures.

H. Social Engineering

Social Engineering is an attack vector performed for penetration testing.

1. Collect information about the target, study the organizational structure, employee names, contacts, etc. Search for public information that can be used to structure an attack.
2. Gain access to target systems or facilities, impersonate employees, vendors, or guests to lure victims into providing information or access permissions. Take advantage of human nature that tends to be cooperative and easy to trust.
3. Increase access rights, after gaining early access, try to upgrade privileges to admin or higher access. For example, by using the Pretexting technique to request an account password update.
4. Avoid detection, Using social engineering to hide intrusion activities from security monitoring.

4. CONCLUSION

Based on the results of penetration testing that has been carried out on the Sibolga City Class 2a District Court web system, the following are the conclusions of the security analysis found,

1. Website security analysis is very important for every government or private agency. There is a web security analysis on finding SQL Injection Vulnerability Loopholes, there are several parameters on web pages that are vulnerable to SQL injection attacks. Attackers can exploit this vulnerability to retrieve sensitive data from databases, such as user information and court documents. Cross-Site Scripting (XSS) vulnerability, where some form inputs are not sanitized properly, making them vulnerable to XSS attacks. Attackers can insert malicious scripts that will be executed by the victim's browser, enabling session theft or defacement of web pages.
2. Lack of Proper Authentication and Authorization with multiple pages accessible without adequate authentication. Unregistered users can access pages and information that should only be accessible to authorized users.
3. Vulnerabilities in Session Management, User sessions are not managed securely, including absence of session time throttling and potential session token leaks. Attackers can steal legitimate user sessions and gain access to the system.
4. Misconfiguration on the Web Server found some configuration files and sensitive information are open for public access. Attackers can leverage this information to carry out follow-up attacks.

REFERENCES

- [1] A. Lubis, E. B. Nababan, and S. Wahyuni, "PENINGKATAN SDM PROMOSI DINAS PARIWISATA SAMOSIR MELALUI PELATIHAN WEBSITE MENGGUNAKAN CMS WORDPRESS," *JMM (Jurnal Masyarakat Mandiri)*, vol. 6, no. 6, pp. 4576–4586, 2022.
- [2] S. Batubara, S. Wahyuni, E. Hariyanto, and A. Lubis, "Webinar Menangkal Cyberporn pada Internet dan Android memanfaatkan add ons dan aplikasi antipornografi parental control di SMA Panca Budi," *Jurnal Abdimas BSI: Jurnal Pengabdian Kepada Masyarakat*, vol. 4, no. 1, pp. 164–173, 2021.
- [3] S. Wahyuni, B. Mesra, A. Lubis, and S. Batubara, "Penjualan Online Ikan Asin Sebagai Salah Satu Usaha Meningkatkan Pendapatan Masyarakat Nelayan Bagan Deli," *Ethos: Jurnal Penelitian dan Pengabdian Kepada Masyarakat*, vol. 8, no. 1, pp. 89–94, 2019.
- [4] S. Wahyuni, A. Lubis, S. Batubara, and I. K. Siregar, "Implementasi algoritma crc 32 dalam mengidentifikasi Keaslian file," in *Seminar Nasional Royal (SENAR)*, 2018, pp. 1–6.
- [5] R. M. Pratama, S. Wahyuni, and A. Lubis, "Rancang Bangun Keamanan Koneksi Pribadi Melalui Open VPN Berbasis Cloud," *INTECOMS: Journal of Information Technology and Computer Science*, vol. 6, no. 1, pp. 30–35, 2023.

- [6] A. Lubis, E. Hariyanto, and M. I. Harahap, "Wireless Controller Menggunakan Capsman di Jaringan Laboratorium Komputer Perguruan Panca Budi Medan," *INTECOMS: Journal of Information Technology and Computer Science*, vol. 5, no. 2, pp. 97–103, 2022.
- [7] A. Lubis, I. Iskandar, and R. Septian, "Pengembangan Aplikasi Troubleshooting Jaringan Melalui Sistem Notifikasi dengan Integrasi Cacti dan Telegram," *Brahmana: Jurnal Penerapan Kecerdasan Buatan*, vol. 4, no. 1A, pp. 104–109, 2022.
- [8] A. Lubis and A. P. U. Siahaan, "Network forensic application in general cases," *IOSR J. Comput. Eng.*, vol. 18, no. 6, pp. 41–44, 2016.
- [9] S. Batubara, E. Hariyanto, S. Wahyuni, I. Sulistianingsih, and N. Mayasari, "Application of Mamdani and Sugeno Fuzzy Toward Ready-Mix Concrete Quality Control," in *Journal of Physics: Conference Series*, IOP Publishing, 2019, p. 012061.
- [10] A. Khaliq, S. Batubara, and M. Syaula, "Designing a Web-Based Career System Using the Laravel Framework," *Jurnal Mantik*, vol. 7, no. 1, pp. 30–38, 2023.
- [11] S. Batubara, "Analisis perbandingan metode fuzzy mamdani dan fuzzy sugeno untuk penentuan kualitas cor beton instan," *IT Journal Research and Development*, vol. 2, no. 1, pp. 1–11, 2017.
- [12] A. Elanda and R. L. Buana, "Analisis Keamanan Sistem Informasi Berbasis Website Dengan Metode Open Web Application Security Project (OWASP) Versi 4: Systematic Review," *CESS (Journal Comput. Eng. Syst. Sci., vol. 5, no. 2, p. 185, 2020, doi: 10.24114/cess. v5i2. 17149, 2020.*
- [13] G. Guntoro, L. Costaner, and M. Musfawati, "Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning)," *JUPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, vol. 5, no. 1, pp. 45–55, 2020.
- [14] A. W. Kuncoro, S. T. Fayruz Rahma, and M. ENG, "Analisis Metode Open Web Application Security Project (OWASP) pada Pengujian Keamanan Website: Literature Review," *Automata*, vol. 3, no. 1, 2022.
- [15] A. Elanda and R. L. Buana, "Analisis Keamanan Sistem Informasi Berbasis Website Dengan Metode Open Web Application Security Project (OWASP) Versi 4: Systematic Review," *CESS (Journal Comput. Eng. Syst. Sci., vol. 5, no. 2, p. 185, 2020, doi: 10.24114/cess. v5i2. 17149, 2020.*
- [16] G. Guntoro, L. Costaner, and M. Musfawati, "Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning)," *JUPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, vol. 5, no. 1, pp. 45–55, 2020.
- [17] S. A. Maulana, "Analisis Keamanan Website dengan Information System Security Assessment Framework (Issaf) dan Open Web Application Security Project (Owasp) di Rumah Sakit Xyz," *Jurnal Indonesia Sosial Teknologi*, vol. 2, no. 04, pp. 506–519, 2021.
- [18] D. Aryanti and J. N. Utamajaya, "Analisis Kerentanan Keamanan Website Menggunakan Metode OWASP (Open Web Application Security Project) Pada Dinas Tenaga Kerja," *Jurnal Syntax Fusion*, vol. 1, no. 03, pp. 15–25, 2021.
- [19] T. Ariyadi, T. L. Widodo, N. Apriyanti, and F. S. Kirana, "Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan OWASP," *Techno. Com*, vol. 22, no. 2, pp. 418–429, 2023.
- [20] I. M. E. Listartha, I. M. A. P. Mitha, M. W. A. Arta, and I. K. W. Y. Arimika, "Analisis Kerentanan Website SMA Negeri 2 Amlapura Menggunakan Metode OWASP (Open Web Application Security Project)," *Jurnal Sistem Informasi dan Sistem Komputer*, vol. 7, no. 1, pp. 23–27, 2022.