P-ISSN : 2715-2448 | E-ISSSN : 2715-7199
Vol.3 No.1 January 2022
*Buana Information Tchnology and Computer Sciences (BIT and CS)*

# SHA512 and MD5 Algorithm Vulnerability Testing Using Common Vulnerability Scoring System (CVSS)

**Fahmi Basya** [1]
Study Program
Information Technology Faculty
Universitas Budi Luhur
1911600482@student.budiluhur.ac.id

**Mardi Hardjanto** [2]
Study Program
Information Technology Faculty
Universitas Budi Luhur
mardi.hardjianto@budiluhur.ac.id

**Ikbal Permana Putra** [3]
Study Program
Information Technology Faculty
Universitas Budi Luhur
2011600364@student.budiluhur.ac.id

***Abstrak*—Tulisan ini membahas perbandingan hasil pengujian algoritma OTP (One Time Password) pada dua enkripsi yaitu SHA512 dan MD5 yang diterapkan pada Aplikasi Rekonsiliasi Dinas Pemberdayaan Masyarakat dan Desa Kabupaten Sukabumi. Studi ini menggunakan metode Vulnerability Assessment and Penetration Testing (VAPT), yang menggabungkan dua bentuk pengujian kerentanan untuk mencapai analisis kerentanan yang jauh lebih lengkap dengan melakukan tugas yang berbeda di area fokus yang sama. Penilaian kerentanan menggunakan metode Common Vulnerability Scoring System (CVSS). Hasil penelitian menunjukkan bahwa metode Vulnerability Assessment and Penetration Testing (VAPT) terbukti mampu mengidentifikasi tingkat kerentanan keamanan pada Aplikasi Rekonsiliasi di Dinas Pemberdayaan Masyarakat dan Desa Kabupaten Sukabumi dengan skor tingkat kerentanan 5,3 pada lingkungan SHA512 dengan peringkat sedang dan 7,5 di lingkungan MD5. dengan peringkat tinggi. Jadi, dapat disimpulkan bahwa algoritma terbaik untuk mengimplementasikan OTP adalah SHA512.***

***Kata Kunci*— OTP, SHA512, MD5, VAPT, CVSS**

***Abstract*—This paper discusses the comparison of the results of testing the OTP (One Time Password) algorithm on two encryptions, namely SHA512 and MD5 which are applied to the Reconciliation Application of the Dinas Pemberdayaan Masyarakat dan Desa Kabupaten Sukabumi. This study uses the Vulnerability Assessment and Penetration Testing (VAPT) method, which combines two forms of vulnerability testing to achieve a much more complete vulnerability analysis by performing different tasks in the same focus area. The vulnerability assessment uses the Common Vulnerability Scoring System (CVSS) method. The results showed that the Vulnerability Assessment and Penetration Testing (VAPT) method was proven to be able to identify the level of security vulnerability in the Reconciliation Application at the Dinas Pemberdayaan Masyarakat dan Desa Kabupaten Sukabumi with a vulnerability level score of 5.3 in the SHA512 environment with a medium rating and 7.5 in the MD5 environment. with high ratings. So, it can be concluded that the best algorithm for implementing OTP is SHA512.**

**Keywords— OTP, SHA512, MD5, VAPT, CVSS**

## I. INTRODUCTION

The Dinas Pemberdayaan Masyarakat dan Desa Kabupaten Sukabumi is a government agency that applies information technology to support daily work processes. The Reconciliation Application which is one of the assets of the Dinas Pemberdayaan Masyarakat dan Desa Kabupaten Sukabumi is a village financial application that functions to control village finances which includes financial input and financial realization. However, at this time, the Reconciliation Application has not implemented a good security system, so application security is currently very vulnerable to cyber-attacks. In addition, to ensure its security, it is necessary to test the system security on the application.

Observing this problem, it is necessary to improve system security by implementing two factor authentication, one of which uses One Time Password (OTP). OTP is an authentication method that uses a password that always changes every login, or changes every certain time interval. It can also be called a password that is only valid for a single login session [1]. The OTP algorithms tested in this study were SHA512 and MD5.

SHA512 is an algorithm that uses a one-way hash function created by Ron Rivest [2] and is a development of the SHA0, SHA1, SHA256, and SHA384 algorithms. The hash itself functions to accept an input string of any length and convert a string whose output length remains the same [3]. The SHA512 algorithm itself is used when generating random codes as an OTP code generator. The SHA512 function produces a message digest with a size of 512 bits and a block length of 1024 bits. In SHA512 there are 80 rounds and for padding bits it is done as in sha-1, but the block size in SHA512 becomes 1024 bits [4]. While the MD5 algorithm was designed by Ron Rivest whose use is very popular among the open-source community as a checksum for downloadable

files [5] which has a block size of 512 bits with a digest size of 128 bits.

The web security testing tool for both SHA512 and MD5 algorithms in this study is the burp suite, which is a Java-based integrated platform for conducting security testing of web applications. Burp suite in general is a web penetration testing framework. This tool is specially made for web applications. Burp suite is now used by most professional testers as part of industry standard penetration tools. In the system security testing process, a combination of two forms of vulnerability testing is used to achieve a much more complete vulnerability analysis by performing different tasks in the same focus area, known as Vulnerability Assessment Penetration Testing (VAPT) [6]. Therefore, in this study, vulnerability testing of the reconciliation application system will be carried out using the VAPT method [9].

## II. METHOD

The research method used is the penetration testing method which refers to a security test framework for a web application system, namely Vulnerability Assessment Penetration Testing (VAPT). VAPT itself is a combination of two Vulnerability Assessment and Penetration Testing activities, where Vulnerability Assessment is an activity that includes the process of examining a security vulnerability of a web application. While Penetration Testing is a process of simulating attacks on vulnerabilities found on the web and exploring them. The testing process using the VATP framework contains 9 necessary stages as shown in the following figure [7].


*Figure 1. VAPT Framework*

Based on Figure 1, this testing phase begins with the scope step (determining the focus of the test, namely information technology assets belonging to the Dinas Pemberdayaan Masyarakat dan Desa Kabupaten Sukabumi, namely the Reconciliation Application), reconnaissance (at this stage information is collected as a basis for targets related to the system will be tested for vulnerability , such as ip address and hosting using domain tools), vulnerability detection (at this stage the process of finding information about security vulnerabilities in the Reconciliation Application using the burp suite tools on the OTP that has been applied is carried out. After finding vulnerabilities, the results are then used as a basis in the planning stage next), information analysis and planning (at this stage analysis and test planning is carried out, namely looking for security vulnerabilities.

This analysis and planning will later be used in the penetration testing process), penetration testing (at this stage sim ulation of attacks on information technology assets of the Dinas Pemberdayaan Masyarakat dan Desa Kabupaten Sukabumi, namely the Reconciliation Application, namely by brute force), privilege escalation (at this stage the vulnerability exploitation process is carried out by utilizing information on vulnerabilities from the results of the penetration testing process), result analysis, reporting and clean-up (at this stage the preparation of a report on the results of the previous stages of testing is carried out). Vulnerability Assessment refers to the standardization of OWASP (Open Web Application Security Project) as well as penetration testing by conducting penetration testing according to standards.

This study then compares the results of the application of the two SHA512 and MD5 algorithms in the Reconciliation Application of the Dinas Pemberdayaan Masyarakat dan Desa Kabupaten Sukabumi through the OTP flow in the figure 2. Based on Figure 2, the flow of the application that will be developed using SHA512 and MD5 to generate a time-based OTP code is synchronized directly with the server in the verification of the OTP code so that it can access into the system. The steps for generating the OTP code are that the user enters the username and password on the login page, then it will be processed by SHA512 or MD5, then the OTP code will be sent to the user's telegram application who will log in [8]. Furthermore, the two algorithms are tested and assessed using the CVSS calculation in table 1 and figure 3 below.

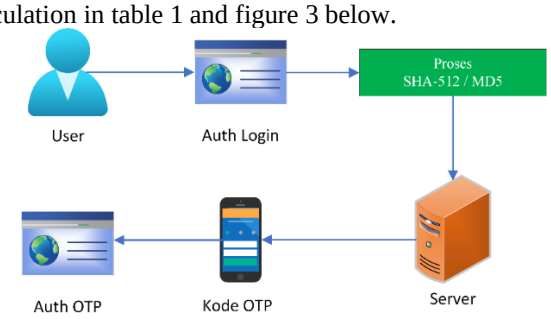


*Figure 2. OTP Flow*

*Table 1. CVSS Score*

| Rating | Base Score |
|---|---|
| **None** | 0,0 |
| **Low** | 0,1 – 3,9 |
| **Medium** | 4,0 – 6,9 |
| **High** | 7,0 – 8,9 |
| **Critical** | 9,0 – 10,0 |

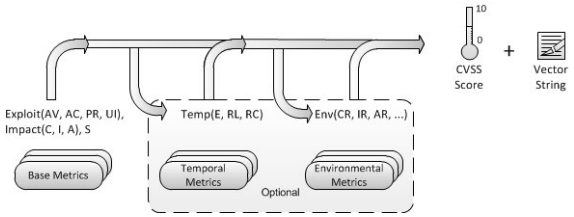


*Figure 3. CVSS Calculation*

**Base score:**
If (Impact sub score <= 0) else, 0)
Scope Unchanged Round up (Minimum [(Impact + Exploitability), 10])
Scope Changed Round up (Minimum [1.08 x (Impact + Exploitability),10])

**Impact sub score**
Scope Unchanged 6.42 x ISCBase
Scope Changed 7.52 x [ISCBase-0.029]-3.25 x [ISCBase-0.02]

**Impact sub score:**
ISCBase = 1 – [(1-ImpactConf) x (1-ImpactInteg) x (1-ImpactAvail)]

**Exploitability sub score:**
8.22 x AttackVector x AttackComplexity x PriviligeRequired x UserInteraction

Vulnerability level testing uses a scoring system from the (CVSS) Common vulnerability Scoring System as a standard for calculating the level of a vulnerability in the system with a vulnerability level value as shown in table 2.

*Table 2. Vulnerability Level of CVSS*

| Rating | Base Score Range |
|---|---|
| **None** | 0,0 |
| **Low** | 0,1 – 3,9 |
| **Medium** | 4,0 – 6,9 |
| **High** | 7,0 – 8,9 |
| **Critical** | 9,0 – 10,0 |

## III. RESULTS AND DISCUSSION

The level scoring test refers to the Common Vulnerability and Exposure (CVE) where CVE is a list that displays any security information, both on software and firmware that are vulnerable to cyber-attacks. This test is done technically to prove the scoring level on vulnerability. After obtaining vulnerabilities for both the SHA512 environment and MD5 algorithms, further testing is carried out on the technical login page (intruder positions process). This test is carried out on the SHA512 environment and MD5 algorithms using tools, namely the burp suite as a scanner as well as the executor, so that the target being analyzed has bugs so that the system can be hacked. Testing the vulnerability of this target using brute force techniques.

*Tabel 3. CVSS Formula SHA512*

| Base Metric | Evaluasi | Skor |
|---|---|---|
| **Attack Vector** | Network | 0,85 |
| **Attack Complexity** | High | 0,44 |
| **Privileges Required** | Low | 0,62 |
| **User Interaction** | None | 0,85 |
| **Scope** | Unchanged | 0,68 |
| **Confidentiality** | High | 0,56 |
| **Integrity** | None | 0 |
| **Availability** | None | 0 |
| **Base Formula** | | |
| **CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N** | | |
| ISS = 1 - [(1-Confidentiality) × (1-Integrity) × (1-Availability)] | | |
| Impact If Scope is Unchanged = 6.42 × ISS | | |
| Exploitability = 8.22 × AttackVector × AttackComplexity × PrivilegesRequired × UserInteraction | | |
| ISS = 1 - [ (1 – 0.56) × (1 - 0) × (1 - 0)] = 1 - (0.44) = 0.56 | | |
| Impact If Scope is Unchanged = 6.42 × 0.56 = 3.6 | | |
| Exploitability = 8.22 × 0.85 x 0.44 x 0.62 x 0.85 = 1.6 | | |
| Impact + Exploitability = 3.6 + 1.6 = 5.3 | | |
| Base Score if scope is unchanged = round up (5.3, 10) = 5.3 | | |

After the intruder positions are executed, the payload sets configuration is then performed, before brute force testing is performed. At this stage, the burp suite will input the possible username and password used. Furthermore, brute force attack testing was carried out on the SHA512 environment and MD5. Then testing the results of the brute force attack on the rendering menu, it appears directly on the OTP page. Furthermore, the configuration of the intruder positions and payload before testing is carried out. The penetration process was successfully carried out by obtaining an OTP code when testing with a brute force attack was carried out. The next process equates the OTP code sent on telegram with the test results on the SHA512 environment and MD5.

The results of testing the SHA512 Environment vulnerability level are presented in table 3 and figure 4.

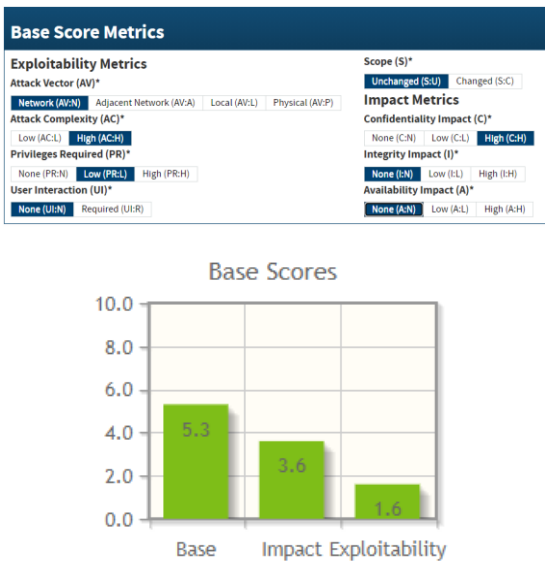


*Figure 4. Base Score Metrics SHA512*

Based on table 3 and figure 4, it is found that the vulnerability level of the SHA512 algorithm is at the medium level.

The results of testing the MD5 vulnerability level can be seen in table 4 and figure 5.

*Tabel 4. CVSS Formula MD5*

| Base Metric | Evaluasi | Skor |
|---|---|---|
| **Attack Vector** | Network | 0,85 |
| **Attack Complexity** | High | 0,44 |
| **Privileges Required** | Low | 0,62 |
| **User Interaction** | None | 0,85 |
| **Scope** | Unchanged | 0,68 |
| **Confidentiality** | High | 0,56 |
| **Integrity** | None | 0,56 |
| **Availability** | None | 0.56 |
| **Base Formula CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N** | | |
| ISS = 1 - [ (1 - Confidentiality) × (1 - Integrity) × (1 - Availability)] Impact If Scope is Unchanged = 6,42 × ISS Exploitability = 8,22 × AttackVector × AttackComplexity × PrivilegesRequired × UserInteraction ISS = 1 - [ (1 – 0,56) × (1 – 0,56) × (1 – 0,56)] = 1 - (0,085) = 0,914 Impact If Scope is Unchanged = 6,42 × 0,914 = 5,9 Exploitability = 8.22 × 0.85 x 0.44 x 0.62 x 0.85 = 1.6 Impact + Exploitability = 5,9 + 1,6 = 7,5 Base Score if scope is unchanged = round up (7,5, 10) = 7,5 | | |

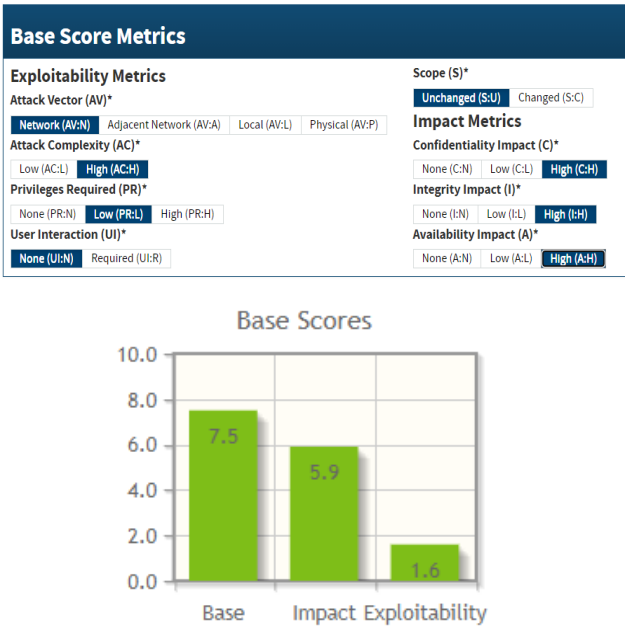





*Figure 5. Base Score Metrics MD5*

Based on Figure 4, it is obtained that Based on Figure 5, it is found that the MD5 Algorithm Vulnerability level is at a high level.

## IV. CONCLUSION

The results of testing security vulnerabilities in the Reconciliation Application of the Dinas Pemberdayaan Masyarakat dan Desa Kabupaten Sukabumi using the Vulnerability Assessment and Penetration Testing (VAPT) method and the blackbox testing approach resulted in the level of vulnerability values being medium in the SHA512 environment and in the MD5 environment with high vulnerability values. From the test results, it is identified that there is a vulnerability in the browser session and the use of an inappropriate hash function, which has the potential to carry out a brute force attack.

## REFERENCES


[1] Perdana, U. P. S. (2016) 'Pemanfaatan Telegram Bot Api Dalam Layanan Otentikasi Tanpa Password Menggunakan Algoritma Time-Based One-Time Password (Totp)', pp. 1–12.

[2] Juardi, D. (2017) 'Kajian vulnerability keamanan data dari eksploitasi hash length extension attack vulnerability data satisfaction study from exploitation hash length extension attack', 6(1)

[3] Rizki, R. and Mulyati, S. (2020) 'Implementasi One Time Password Menggunakan Algoritma SHA-512 Pada Aplikasi Penagihan Hutang PT. XHT', *Edumatic : Jurnal Pendidikan Informatika*, 4(1), pp. 111–120. doi: 10.29408/edumatic.v4i1.2158.

[4] Sembiring, J. (2013) 'Analisis Algoritma Sha-512 Dan Watermarking Dengan Metode Least Significant Bit Pada Data Citra', *Seminar Nasional Sistem Informasi Indonesia*, pp. 2–4.

[5] Sulastri, S. and Putri, R. D. M. (2018) 'Implementasi Enkripsi Data Secure Hash Algorithm (SHA-256) dan Message Digest Algorithm (MD5) pada Proses Pengamanan Kata Sandi Sistem Penjadwalan Karyawan', *Jurnal Teknik Elektro*, 10(2), pp. 70–74. doi: 10.15294/jte.v10i2.18628

[6] Simran, G. and Sasikala, D. (2019) 'Vulnerability Assessment of Web Applications using Penetration Testing', *International Journal of Recent Technology and Engineering*, 8(4), pp. 1552–1556. doi: 10.35940/ijrte.b2133.118419.

[7] Goel, J. N. and Mehtre, B. M. (2015) 'Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology', *Procedia Computer Science*, 57, pp. 710–715. doi: 10.1016/j.procs.2015.07.458.

[8] Setiawan, D. A. *et al.* (2018) 'Implementasi One Time Password Menggunakan Algoritma Hash Sha-512 Berbasis Web Pada Badan Kepegawaian Dan Pengembangan Sdm Kota', *Skanika Volume 1 No. 1 Maret 2018 Implementasi*, 1(1), pp. 199–204.

[9] D. Kurniawan, A. L. Hananto, and B. Priyatna, "Modification Application of Key Metrics 13x13 Cryptographic Algorithm Playfair Cipher and Combination with Linear Feedback Shift Register (LFSR) on Data Security Based on Mobile Android," *Int. J. Comput. Tech.*-–, vol. 5, no. 1, pp. 65–70, 2018.

[10] B. Huda, "Sistem Informasi Data Penduduk Berbasis Android Dan Web Monitoring Studi Kasus Pemerintah Kota Karawang (Penelitian dilakukan di Kab. Karawang)," Buana Ilmu, vol. 3, no. 1, pp. 62–69, 2018, doi: 10.36805/bi.v3i1.456.