Indonesian Journal of Community Engagement
Jurnal Pengabdian kepada Masyarakat
Vol. 9, No. 3, September 2023, Page. 158-162
DOI: http://doi.org/10.22146/jpkm.80089

# Application Security Testing to Support Digital-Based Cultural Ecosystem in Jogja Smart Province

**Sahirul Alam*, Sri Lestari, Budi Bayu Murti, Nur Rohman Rosyid, Ronald Adrian, Anni Karimatul Fauziyyah, Muhammad Hamdan, Josua Rusdi Hutagaol, Sakhiya Abida, Ingrid Rorez Dialusi Sinurat**

Department of Electrical Engineering and Informatics, Vocational College, Universitas Gadjah Mada, Yogyakarta, Indonesia

Submitted: December 12th 2022; Revised: August 24th 2023; Accepted: August 25th 2023

**Keywords:**
Application penetration testing
Cyber-attack
Information security
Jogja smart province

**Abstract** The Jogja Smart Province (JSP) is a framework for using IT to encourage regional cooperation to assist in resolving specific strategic challenges or difficulties. Additionally, JSP supports the growth of potential in Yogyakarta's Special Region. Several digital apps, including mobile and web-based ones, support JSP. These applications are crucial to actualizing the five JSP aspects of smart living, culture, society, environment, and governance. However, several significant issues, such as cyberattacks on JSP applications, pose a danger to the long-term viability of JSP. To do penetration testing of JSP-owned applications, the Department of Electrical Engineering and Informatics at the Vocational College of Universitas Gadjah Mada is conducting this community participation initiative. The Communication and Informatics Office of the Special Region of Yogyakarta permitted to handle JSP apps, is a partner in this community involvement initiative. Applications including Jogja Istimewa, Visiting Jogja, e-Prima, BiroHukum, Paperless, Jogjaplan, LPSE, Peladen, Sadewa, Jogjaprov, and Simpeg2 are among those targeted for penetration testing. The potential flaws detected in JSP applications can be found by performing penetration testing on these apps. In addition, several recommendations are made to strengthen JSP applications' resistance to future cyberattacks. Therefore, this activity can improve the security of the users' data and directly impact the community.

## 1. INTRODUCTION

Information technology has been developed significantly up to now and it has been implemented in all fields around us. One area that has implemented the advances in information technology is the government and hence the concept of smart governance emerges. Meanwhile, smart governance itself is one of the dimensions of a smart city that embraces all aspects related to government and community services and is related to local administration (Lopes, 2017). The concept of smart governance is starting to be applied in various cities in the world. In Indonesia, one of the cities or regions that applies this concept is the province of the Special Region of Yogyakarta or Daerah Istimewa Yogyakarta (DIY). The concept of smart governance was launched by the DIY provincial government under the name of Jogja Smart Province (JSP) (Diskominfo DIY, 2022).

JSP is a regional collaboration based on information technology to support the resolution of strategic issues and potential development in the Special Region of Yogyakarta. JSP has five dimensions as follows: smart living, smart culture, smart society, smart environment, and smart governance. To support the realization of the five dimensions of the JSP, various applications were made. One

ISSN 2460-9447 (print), ISSN 2541-5883 (online)
*Corresponding author: Sahirul Alam
Department of Electrical Engineering and Informatics, Vocational College, Universitas Gadjah Mada, Sekip Unit III, Yogyakarta, Indonesia, 55281
Email: sahirul.alam@ugm.ac.id

of these applications is Jogja Istimewa which is a mobile application that covers 97% of Yogyakarta itself which is so special (Diskominfo DIY, 2022). The main features presented are information about the city of Yogyakarta such as tourist attractions, hotels and inns, shopping centers, cultural heritage encyclopedias, handicraft products, culinary, public services, flight schedule information, interesting event schedules to TV and CCTV streaming in Yogyakarta.

Many applications have been developed to support JSP in various fields. The application has been widely used and utilized by the residents of Yogyakarta and the DIY government itself. The application is also used by anyone, especially those who visit Yogyakarta. In addition to the benefits provided by these applications, there are important things that need to be considered, namely information security, especially for application users. However, there are many cyber-attacks targeting JSP applications based on the log data owned by the Communications and Informatics Office (KOMINFO) of DIY. This is a serious problem since it can threaten information security (Lee et al., 2016) as well as threaten the digital resilience of JSPs. Therefore, this community engagement activity focuses on this problem.

Based on the problems that have been described previously, this community engagement activity has the following objectives.

1. to perform penetration testing toward some applications owned by JSP
2. to evaluate the vulnerabilities of JSP applications
3. to provide recommendations for improving the security of JSP applications
4. to improve the data security of the users as the direct impact on the community

Penetration testing or pen-test or ethical hacking is a simulation of a cyber-attack on a computer system with the authorization of the owner of the attack target. Pen-test aims to evaluate the security system of the application (Pohan et al., 2021). Through penetration testing, the weaknesses of the application (also known as vulnerabilities) can be identified, including the potential access to data and system features by unauthorized parties (Henry, 2012).

There have been several works related to penetration testing. However, most of those works were targeting web-based applications. The methods used for penetration testing are SQL injection (Bastian et al., 2020), dynamic application security testing (DAST) (Wicaksono et al., 2020), and input validation testing (Hanafi et al., 2019). In this community engagement, penetration testing was not only targeting web-based applications but also Android-based applications.

# 2. METHOD

## 2.1 Time and location

This community service program consists of several activities. The activity began with a penetration testing training which was held on 1$^{st}$ July 2022 at the RPL 9 Laboratory, Department of Electrical Engineering and Informatics (DTEDI), Vocational College, Universitas Gadjah Mada (UGM). The series of penetration testing activities itself was carried out from 4$^{th}$ July 2022 to 19$^{th}$ August 2022. Penetration testing of the application was carried out at the TAJ Laboratory of DTEDI during a certain allocated time. In addition, there were meetings to report the progress of penetration testing activities with the partner which were carried out online through the Zoom meeting application. Progress reporting meetings were held twice on 15$^{th}$ July and 15$^{th}$ August 2022. The community engagement program was closed with a mini workshop to expose the results of penetration testing and discussions with partner held at the KOMINFO DIY Office on 9$^{th}$ September 2022.

## 2.2 Target of activity

The applications that became the target of this community engagement activity are applications that are included in the Jogja Smart Province and are managed by the KOMINFO of DIY. There were eleven applications tested consisting of three Android-based mobile applications and eight web-based applications. Android-based applications include Visiting Jogja, Jogja Istimewa, and e-Prima. While web-based applications include Peladen, Sadewa, Jogjaprov, Simpeg2, Paperless, LPSE, Biro Hukum, and JogjaPlan.

## 2.3 Application security testing method

This community engagement activity is carried out by conducting penetration testing of applications owned by JSP. After penetration testing, the security vulnerability findings of each application are documented in a typical penetration testing report format. The penetration testing results are submitted to the community engagement partner to be used to improve the security of JSP applications.

The penetration testing method itself is divided into two according to the type of application. Penetration testing for Android applications consists of several stages as follows.

1. Reverse engineering of Android application

   Reverse engineering is performed to get the source code of the application. Thus, the mechanism of the application can be studied. In addition, the source code is also used as an initial asset to analyze the security vulnerabilities of the application. Some of the tools that can be used to reverse engineer Android applications include JADX, APKTool, dex2jar, and so on. The success indicator of this stage is the acquisition of the application source code.

2. The exploitation of android application components

   The exploitation of application components aims to perform a security-level analysis of the application. The analysis can be done using static or dynamic methods. One of the tools that can be used to exploit application components using both static and dynamic methods is the Mobile Security Framework,

also known as MobSF. The success indicator of this stage is the report of the testing result defining the security level of certain aspects of the application.

3. Android apps traffic analysis

   Application security vulnerabilities can also be carried out by analyzing data traffic on the application. Tools that can be used for traffic analysis include Drozer, developed by MWR Labs. The success indicator of this stage is the report of traffic analysis.

4. The practice of Android apps vulnerabilities

   The success indicator of this stage is the report presenting the vulnerabilities findings.

Penetration testing for web-based applications can be done by using tools such as arachni, wapiti, and w3af (Tarigan et al., 2017). In this community engagement, the web pen-test is carried out using paid tools. This is done with several considerations. The first is due to the limited time for the implementation of the activities compared to the number of applications to be tested. The second is to obtain more optimal penetration testing results for web-based applications. Thus, the team members can focus on penetration testing for Android applications, so that pen-test results for Android applications are also more optimal. Pen-testing of the web application was carried out using a tool from pentest-tools.com. The pen-test tools provided by the platform include the following.

1. Website vulnerability scanner

   This tool is used to test for vulnerabilities that affect web applications such as SQL Injection, XSS, OS Command Injection, Directory Traversal, and so on. The scanning process can also be used to find specific problems with web server configuration.

2. XSS scanner

   XSS scanner is used to test the resilience of web applications against Cross-Site Scripting attacks.

3. SQLi injection scanner

   This tool is used to find web application vulnerabilities to SQL injection by performing in-depth inspections of a web page and its parameters.

### 2.4 Deliverable

The deliverable of this activity is the completion of penetration testing of eleven applications that have been agreed upon by the team and partner. In addition, the completion of this activity is also indicated by the documentation of penetration testing results in a standard format. The documentation includes the vulnerability finding summary as shown in Table 1, 2, and 3 (3S Labs, 2022) and several suggestions to solve the vulnerabilities.

### 2.5 Evaluation method

The monitoring and evaluation of this activity is carried out through the meetings between team members and partner. There are two types of meetings held for evaluation and monitoring, namely progress report meetings and mini workshop meetings. In the progress report meeting, in addition to the progress of penetration testing results, the obstacles encountered during the activity were also discussed. Thus, both team members and partner can provide input to overcome obstacles or design further activities. In the second meeting, namely a mini workshop, the results of penetration testing were presented to the partner in the form of presentations and discussions. Thus, the partner gets clearer information regarding the results of penetration testing while at the same time having the opportunity to share penetration testing methods and solutions to improve the security of applications that have been tested.

Table 1 . Vulnerability summary

| Risk Ratings | Number of findings |
|---|---|
| Critical | 2 |
| High | 5 |
| Medium | 3 |
| Low | 11 |
| **Total** | 21 |

Table 2 . Total risk per target

| System | Field of application | Risk |
|---|---|---|
| www.example.com | http/web | High |

Table 3 . Vulnerability risk ratings

| System | Field of application | Risk |
|---|---|---|
| Cross-site scripting | Web1 | High |
| SQL Injection | Web1 | High |

## 3. RESULT AND DISCUSSION

As previously explained, this community engagement activity consists of several sub-activities, namely pen-test training for the student members of the team, inaugural meeting with the partner, penetration testing of JSP applications, progress reports, and mini workshop. The discussion of the results of each of these sub-activities is as follows.

### 3.1 Android app penetration testing training for students

This training aims to prepare the students with the skill to perform penetration testing of Android-based mobile applications. The training was held in the RPL 9 Laboratory of DTEDI on 1$^{st}$ July 2022. The trainer for this event was one of the lecturers who was a member of the team. The results or output of this activity are as follows.

1. Students have the provision expertise in penetration testing Android applications so that later they can be directly involved in community engagement activities.
2. This training has never been done before, so there is a side output from the training activity, namely

the preparation of an Android application penetration testing training module.

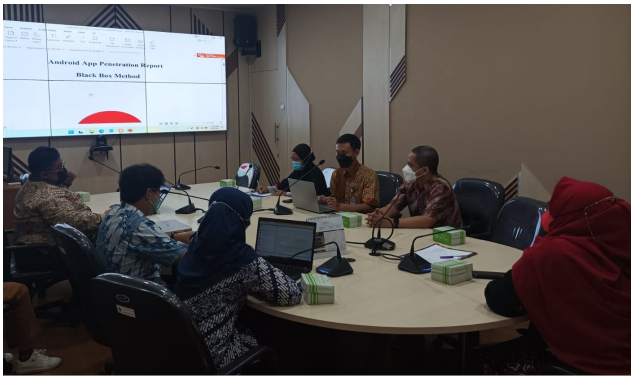


Figure 1 . Mini-workshop on penetration testing results

### 3.2 Inaugural meeting with the partner

Figure 1 shows the first meeting with the community engagement partner which was held at the KOMINFO DIY Office at Jalan Brigjen Katamso Yogyakarta on 4th July 2022. The meeting was attended by the community engagement members, staff, and the head of the Information Security and Encryption Service for KOMINFO DIY. The purpose of this meeting is to discuss the technical implementation of the community engagement activities and the agreement regarding the applications that become the target of penetration testing. As a result, eleven applications had been approved to become the target of penetration testing, as mentioned in the previous section. Moreover, the duration of penetration testing activity was also determined as stated in the previous section.

### 3.3 Penetration testing activity progress report

Progress report meetings are held to discuss the progress of the penetration testing activities and the obstacles encountered. In addition to monitoring so that activities can be carried out by the activity timeline plan, the partner can also provide feedback or suggestions regarding the progress of activity results and subsequent plans. Notes on the pen-test activity progress report are as follows.

1. First Progress Report, July 15, 2022, online Zoom.
    a. Several stages of penetration testing had been carried out for Android-based applications, namely: information gathering including APK download, decompile, root bypass, recompile, and penetration testing with Kali Linux to check vulnerability status.
    b. The android applications that were the target of the pen-test are Visiting Jogja, Jogja Istimewa, and e-Prima.
    c. The report format was not well documented, it was recommended to use the OWASP report format.
2. Second Progress Report, August 15, 2022, online Zoom.
    a. Improvement of the previous pen-test results report had been done.
    b. The results of the web application pen-test (using the pen-test tool) had been exposed.
    c. The planning of a mini-workshop event was discussed.

Reports on the findings of penetration testing are categorized into several levels of vulnerability, namely Low, Medium, and High. Categorization is done using the standards from the Open Web Application Security Project (OWASP) (OWASP, 2022). Penetration testing results cannot be shown to the public. However, as an illustration, the summary of the vulnerability categorization is shown in Table 1, 2, and 3 (3S Labs, 2022).

### 3.4 Mini workshop and closing

The mini-workshop event was held at the KOMINFO DIY Office on 9th September 2022. In the mini-workshop as depicted in Figure 1, the results of penetration testing of eleven applications that had been agreed upon as the pen-test targets were presented. Furthermore, a discussion regarding the results of the pen-test was carried out with the partner. In addition, the documentation of pen-test results in the form of soft file reports was also delivered to the partner. However, the documentation of pen-test results is confidential, thus it cannot be published or shown to the public. The results of penetration testing were expected to be useful for the partner to improve the security and the sustainability of applications owned by JSP. Furthermore, the resilience of the JSP application can improve the security of users' data as the direct impact of this activity on the community. Finally, the end of this workshop also formally closed the community engagement activities.

## 4. CONCLUSION

The main activity of this community engagement is the penetration testing of applications owned by Jogja Smart Province which consists of three Android-based applications and eight web-based applications. Application penetration testing is carried out to find out the vulnerabilities or security risks of these applications. With the vulnerability findings, the Communications and Informatics Office of DIY as the partner of community engagement as well as the institution in charge of managing the JSP application can develop a plan to improve the application security. Thus, JSP applications are expected to have better resilience against various cyber-attacks potential and the security of the users' data can be improved so that this activity can give benefit to the community.

Suggestions that can be given to the parties who wish to carry out similar activities are as follows. First, the better the infrastructure used, the more convenient penetration testing activities can be. For example, the use of licensed virtual machines will be better than freeware, especially in terms of computational speed and pervasive capabilities. Furthermore, further exploration needs to be carried out so that it can provide better recommendations and more

appropriate solutions to be used by partner with various considerations.

## ACKNOWLEDGMENT

This community engagement activity is supported by the Vocational College of Universitas Gadjah Mada through Pelaksanaan Pengabdian Masyarakat Dana Masyarakat Sekolah Vokasi Program Year 2022, with the grant number 206/UN1.SV/K/2022. Furthermore, the Authors would like to thank the partner of this community engagement, the Communications and Informatics Office (Dinas Komunikasi dan Informatika) of the Special Region of Yogyakarta.

## CONFLICT OF INTERESTS

The Authors of this article entitled “Application Security Testing to Support Digital-Based Cultural Ecosystem in Jogja Smart Province" declare no conflict of interest. Additionally, the contact person is the corresponding author who will communicate with the representative of JPKM in the editorial process until it is published

## REFERENCES

3S Labs. (2022). *Web application penetration testing*. https://www.3slabs.com/web-application-penetration-testing.php

Bastian, A., Sujadi, H., & Abror, L. (2020). Analisis keamanan aplikasi data pokok pendidikan (DAPODIK) menggunakan penetration testing dan SQL injection. *INFOTECH journal*, 65-70.

Diskominfo DIY. (2022). *Jogja istimewa apps*. https://diskominfo.jogjaprov.go.id/layanan/lihat/jogja-istimewa-apps

Diskominfo DIY. (2022). *Jogja smart province - development plans*. https://jsp.jogjaprov.go.id/p/6-development-plans

Hanafi, T. A., Iswahyudi C., & Rachmawati, R. Y. (2019). Aplikasi pendeteksi celah keamanan aplikasi web dengan penetration testing menggunakan metode input validation. *Jurnal SCRIPT*, 132-141.

Henry, K. M. (2012). *Penetration testing: Protecting networks and systems*. IT Governance Ltd.

Lee, H., Kwon, E., Yoo, K., & Chai, S. (2016). An impact of information security investment on information security incidents: A case of Korean organizations. *ACM International Conference Proceeding Series*,1-4.

Lopes, N. V. (2017). Smart governance: A key factor for smart cities implementation. *International Conference on Smart Grid and Smart Cities*, 277-282.

OWASP. (2022). *About the OWASP foundation*. https://owasp.org/about/

Pohan, Y. A., Yunus, Y., & Sumijan. (2021). Meningkatkan keamanan webserver aplikasi pelaporan pajak daerah menggunakan metode penetration testing execution standar. *Jurnal Sistim Informasi dan Teknologi*, 1-6.

Tarigan, B. V., Kusyanti, A., & Yahya, W. (2017). Analisis perbandingan penetration testing tool untuk aplikasi web. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 206-214.

Wicaksono, B., Kusumaningsih, R. Y., & Iswahyudi, C. (2020). Pengujian celah keamanan aplikasi berbasis web menggunakan teknik penetration pesting dan DAST (Dynamic Application Security Testing). *Jurnal Jarkom*, 1-9.