

Security system testing on electronic integrated antenatal care (e-iANC)

Hosizah, Fachmi Tamzil

Department of Health Information Management, Faculty of Health Sciences, Universitas Esa Unggul, Indonesia

Article Info

Article history:

Received Nov 19, 2018

Revised Apr 29, 2019

Accepted Jul 17, 2019

Keywords:

Antenatal care (ANC)

Electronic integrated antenatal care (e-iANC)

Electronic medical records (EMR)

Open web application security project (OWASP)

ABSTRACT

Electronic Integrated Antenatal Care (e-iANC) was built as a web-based application to assist midwives in recording Antenatal Care (ANC) data including Patient Registration; Anamnesis; Physical Examination; Laboratory Test, Screening of Risk Pregnancy; Communication, Information and Education; Treatment and follow-up; Patient Disposition. To ensure e-iANC becomes a safe system, security system testing was needed. Our goals were to test the security system by using the Open Web Application Security Project (OWASP). It was conducted in computer laboratory at Universitas Esa Unggul Jakarta in August 2017. The OWASP detect include Injection, Broken Authentication and Session Management, Cross-Site Scripting (XSS), Insecure Direct Object References, Security Misconfiguration, Sensitive Data Exposure, Missing Level Access Control, Cross Site Request Forgery (CSRF), Using Known Vulnerable Components, Unvalidated Redirects and Forwards. The results indicated the risk level of e-iANC was the low category in the aspect of Cross-Domain JavaScript Source File Inclusion, Private IP Disclosure, XSS Protection Not Enabled Web Browser.

*Copyright © 2020 Institute of Advanced Engineering and Science.
All rights reserved.*

Corresponding Author:

Hosizah,

Department of Health Information Management,

Faculty of Health Sciences, Universitas Esa Unggul,

Arjuna Street No.9, Kebon Jeruk, West Jakarta 11410, Indonesia.

Email: hosizah@esaunggul.ac.id

1. INTRODUCTION

In 2012, the Indonesian Maternal Mortality Ratio (MMR) was 359 per 100,000 live births [1, 2]. This is very high when compared to neighboring countries, such as Singapore (3 per 100,000 live births), Malaysia (5 per 100,000 live births), Thailand (8-10 per 100,000 live births), and Vietnam (50 per 100,000 live births) [3]. Indonesian MMR is far above the target Millennium Development Goals (MDGs) of 102 per 100,000 live births in 2015 [4, 5]. The Indonesian MMR has also increased in recent years, from 307 per 100,000 in 2002 to 359 per 100,000 in 2012 [4]. This increase happened in spite of improvements in coverage over the same period in obstetric care (92%-98%); delivery by healthcare provider (66%-83%); and delivery in health care facilities (40%-63%).

Healthcare providers must be able to ensure that the pregnancy is normal, to detect early problems and illnesses, and to intervene adequately so that pregnant women are ready to undergo a normal delivery. Antenatal Care (ANC) services provided by Indonesian midwives include taking vital measurements, assessing nutritional status, measuring fundal height, assessing the presentation of fetus and Fetal Heart Rate (FHR), screening for tetanus toxoid immunization status and giving tetanus toxoid if needed, dispensing Iron supplements (Fe tablets), ordering laboratory tests (routine and special), managing cases, and counseling [4]. Midwives must complete several forms to the provision documents of Integrated ANC, including basic medical records, detailed pregnancy-related information known as a "Mother Card", the "Mother and Child

Health Handbook” (a record provided to the mother), public health reporting forms used for local and national monitoring known as a “Mother Cohort”, and District Health Reports. Data on these paper forms often incomplete and/or inaccurate, thus limiting possibilities for quality improvement analyses [4].

Our interviews identified several difficulties with the paper-based Integrated Antenatal Care (ANC) processes at primary health center in Bangkalan, including: redundancy in ANC data leading to inconsistencies; difficulties in using and interpreting paper records leading to delay on risk screening and service interventions; delay in accessing data; and inaccurate calculation and data analysis. Participants found the integrated ANC forms to be burdensome and redundant. Some felt that completion of the forms interfered with providing necessary antenatal care. In fact, many health information systems did not retain the real data in the form of an individual patient record. Instead the data are collected in the form of patients total summary which was obscuring the individual patient history and make it difficult to follow patients record over time [6-10].

Electronic Integrated Antenatal Care (e-iANC) was built as a web-based application to assist midwives in recording ANCs data including Patient Registration; Anamnesis; Physical Examination; Laboratory Test, Screening of Risk Pregnancy; Communication, Information and Education; Treatment and follow-up; Patient Disposition [6].

A web-based application (include e-iANC) is a media which is containing many informations that can be accessed quickly and freely by the public [11-13]. This condition made it difficult to prevent the introduction of vulnerability, and limited skills and lack of security culture. All these factors web applications more vulnerable and exploitable by hackers. In addition, network security and the installation of firewalls lack to provide adequate protection against Web-based attacks [14-17].

Several communities were born with the aim of improving the security of web applications, one of them is Open Web Application Security Project (OWASP) [18]. To ensure e-iANC becomes a safe system, security system testing was needed. This study aimed to test the security level of e-iANC web-based application by using the OWASPZAP.

2. RESEARCH METHOD

The website security vulnerability testing was conducted using Open Web Application Security Project Zed Attack Proxy (OWASPZAP) with 4 parameters of vulnerability levels including Informational, Low, Medium and High.

OWASP as an open source community dedicated to develop and maintain a web-based application and released top 10 risk components include Injection, Broken Authentication and Session Management, Cross-Site Scripting (XSS), Insecure Direct Object References, Security Misconfiguration, Sensitive Data Exposure, Missing Level Access Control, Cross Site Request Forgery (CSRF), Using Known Vulnerable Components, Unvalidated Redirects and Forwards [13].

The GET method used in this OWASPZAP test (to e-iANC web-apps) with the scheme in Figure 1.



Figure 1. OWASPZAP test scheme on e-iANC

As shown in Figure 1, the OWASP application used as a media to scan and detect the security level of an e-iANC website. The URL of e-iANC will be inserted over the process it will give the result.

3. RESULTS AND ANALYSIS

The OWASPZAP application will be released the results in the form of tables. The top table contains the risk level of the security gap, the number of loopholes that can be detected and the next table contains the level of risk gap, the category or name of the gap, the location of the gap, the last method, parameters and tables containing solutions to security holes. In this study the possibility of an attack used consisted of 3 attacks as shown in Table 1.

Table 1. Probability attacks

No	Target (Possibility of an Attack)
1	Cross Domain Javascript Source File Inclusion
2	Private IP Disclosure
3	Web Browser XSS Protection Not Enabled

All of that possibility of an attack in the e-iANC web-apps have been examined with the result. Table 2 shows vulnerability (security gap) reports of cross domain Javascript source file inclusion and Figure 2 shows the solution to handling that.

Table 2. Vulnerability (security gap) reports of cross domain javascript source file inclusion

URL	Method	Parameter	Evidence
		https://www.googletagservices.com/tag/js/gpt.js	<script async='async' src='https://www.googletagservices.com/tag/js/gpt.js'></script>
		https://assets.mobicast.io/widget/main.js	<script src="https://assets.mobicast.io/widget/main.js"></script>
		https://cdn.uzone.id/assets/mercusuar/js/jquery-2.2.4.min.js	<script type="text/javascript" src="https://cdn.uzone.id/assets/mercusuar/js/jquery-2.2.4.min.js"></script>
		https://cdn.uzone.id/assets/mercusuar/strap-3.3.7-dist/js/bootstrap.js	<script type="text/javascript" src="https://cdn.uzone.id/assets/mercusuar/strap-3.3.7-dist/js/bootstrap.js"></script>
		//pagead2.googlesyndication.com/pagead/show_ads.js	<script type="text/javascript" src="//pagead2.googlesyndication.com/pagead/show_ads.js"></script>
		http://cdn.uzone.id/assets/js/script-2.js	<script type="text/javascript" src="http://cdn.uzone.id/assets/js/script-2.js"></script>
http://e-ianc.com	GET	https://das.uadexchange.com/ads/www/delivery/ads.js?zoneid=1191	<script type='text/javascript' src='https://das.uadexchange.com/ads/www/delivery/ads.js?zoneid=1191'></script>
		http://js.digiads.co.id/t/111/579/a1111579.js	<script type="text/javascript" src="http://js.digiads.co.id/t/111/579/a1111579.js"></script>
		//pagead2.googlesyndication.com/pagead/show_ads.js	<script type="text/javascript" src="//pagead2.googlesyndication.com/pagead/show_ads.js"></script>
		https://cdn.uzone.id/assets/mercusuar/js/responsiveCarousel.js	<script type="text/javascript" src="https://cdn.uzone.id/assets/mercusuar/js/responsiveCarousel.js"></script>
		http://js.genieessp.com/t/081/689/a1081689.js	<script type="text/javascript" src="http://js.genieessp.com/t/081/689/a1081689.js"></script>
		//pagead2.googlesyndication.com/pagead/show_ads.js	<script type="text/javascript" src="//pagead2.googlesyndication.com/pagead/show_ads.js"></script>
		//st-n.ads1-adnow.com/js/adv_out.js	<script type="text/javascript" src="//st-n.ads1-adnow.com/js/adv_out.js"></script>

Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Source ID	3

Figure 2. Solution on handling the vulnerability of cross domain javascript source file inclusion

Figure 3 and Figure 4 show the vulnerability report of private IP disclosure and solution on handling that vulnerability.

Low (Medium)	Private IP Disclosure
Description	A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.
URL	http://e-ianic.com
Method	GET
Evidence	172.17.60.43
Instances	1

Figure 3. Vulnerability report of private IP disclosure

Solution	Remove the private IP address from the HTTP response body. For comments, use JSP/ASP/PHP comment instead of HTML/JavaScript comment which can be seen by client browsers.
Other information	172.17.60.43
Reference	https://tools.ietf.org/html/rfc1918
CWE Id	200
WASC Id	13
Source ID	3

Figure 4. Solution on handling vulnerability on private IP disclosure

Figure 5 shows vulnerability report on web browser XSS protection not enabled and Figure 6 shows the solution of that report.

Low (Medium)	Web Browser XSS Protection Not Enabled
Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
URL	http://e-ianic.com
Method	GET
Parameter	X-XSS-Protection
Instances	1

Figure 5. Vulnerability report on web browser XSS protection not enabled

Solution	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.
Other information	<p>The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it:</p> <p>X-XSS-Protection: 1; mode=block</p> <p>X-XSS-Protection: 1; report=http://www.example.com/xss</p> <p>The following values would disable it:</p> <p>X-XSS-Protection: 0</p> <p>The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit).</p> <p>Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).</p>
Reference	<p>https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet</p> <p>https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/</p>
CWE Id	933
WASC Id	14
Source ID	3

Figure 6. Solution on handling the vulnerability of web browser XSS protection not enabled

Electronic Integrated Antenatal Care (e-iANC) has been examined by using the OWASPzap top 10 and given the result in Figure 7. The Figure 7 shown that the vulnerability risk level of e-iANC categorized as a Low Risk Level which represented by number 3. It means the security gaps detected do not endanger the web at <http://e-ianc.com>. Based on the research for every vulnerability or security gap, given a solution as written in Table 3.

Risk Level	Number of Alerts
High	0
Medium	0
Low	3
Informational	0

Figure 7. Risk level of e-iANC vulnerability

Table 3. Solutions to handle the vulnerabilities or security gaps

Security Gaps or Vulnerabilities	Solution
Cross Domain Javascript Source File Inclusion	Ensure that javascript files are only loaded on the trusted sources and the sources cannot be controlled by the last users
Private IP Disclosure	Erase the personal IP address from body HTTP. To comment use only JSP/ASP/PHP not HTML / Javascript that can be seen by client browser
Web Browser XSS Protection Not Enabled	Ensure that XSS filter browser web is activated by controlling header response on HTTP X-XSS-Protection to '1'

Features of e-iANC

Electronic Integrated Antenatal Care (e-iANC) is being an implementing of Electronic Medical Records (EMR). An electronic medical record is a real-time patient health record with access to evidence-based decision support tools that can be used to aid clinicians on making the decisions [19-22]. The EMR can automate and streamline a clinician's workflow, ensuring that all clinical information is well-communicated. It also prevent the delay in response that would make the gaps in care. Moreover, The EMR can support the collection of data for uses other than clinical care, such as billing, quality management, surveillance and reporting the public health diseases [23-25].

Below are the features of e-iANC:

- a. Patient Registration: enabling entry of demographic and financial sources data, including whether a patient pays in cash or is financed by the Healthcare and Social Security Agency [23].
- b. Anamnesis, including history of current or previous pregnancy as well as labor history, as needed to identify high-risk patients. The first day of the last menstrual period is used to estimate the expected date of birth (Figure 2).
- c. Physical Examination: results of physical examinations, including vital signs used to detect early pregnancy risks such as of CPD, Preeclampsia, etc [4].
- d. Laboratory test: Urine protein; HBs Ag; BTA etc., as medically indicated.
- e. Screening of Risk Pregnancy, described as low, high, or very high risk [26].
- f. Communication, Information and Education (CIE): Education materials related to factors such as delivery planning; nutritional problems; tetanus toxoid immunization; HIV/AIDS and other communicable diseases; exclusive breastfeeding, brain booster etc.
- g. Treatment and follow-up: key treatments administered, including injection of tetanus toxoid and the e provision of multivitamins. Midwives can enter the number and doses defined and administration instructions.
- h. Patient Disposition: follow-up instructions including discharge or referral if necessary to other healthcare provider or health care facilities with more complete equipment.
- i. Diagnosis: Entry of specific antenatal diagnosis, using ICD-10 codes as required to process claims-reimbursement [27].
- j. Graphics of the maternal weight and Body Mass Index (BMI), can be used to monitor maternal weight before for each visit. This novel visualization of health information was seen as necessary to expedite.
- k. Reports: display and printing of Mother Cohort and District Health Reports on rural and primary health centers. Reports are available both to midwives and to the head of primary health center.

4. CONCLUSION

Electronic Integrated Antenatal Care (e-iANC) is an innovation which is combining *electronic medical record* and web-based. Therefore with only one entry of Antenatal Care (ANC) data, midwives can access real-time individual and aggregate health information of pregnant women. This can be employed for clinical service and organization decision making; research; performance improvement; and education. The results indicated the risk level of e-iANC was the low (which is represented by number 3) category in the aspect of Cross-Domain JavaScript Source File Inclusion, Private IP Disclosure, XSS Protection Not Enabled Web Browser.

ACKNOWLEDGEMENTS

We thank the Directorate General of Higher Education, Ministry of Research Technology and Higher Education Indonesia on grant for applied research entitled success adoption model on electronic integrated antenatal care.

REFERENCES

- [1] Statistics Indonesia (BPS), National Population and Family Planning Board (BKKBN), and Ministry of Health (Kemenkes), and ICF International, "Indonesia Demographic and Health Survey 2012," Jakarta, Indonesia, BPS, BKKBN, Kemenkes, and ICF International, 2013.
- [2] Ministry of Health, Republic of Indonesia, "Ministry of Health Release RAN-PPAKI 2013-2015, RAN-PPIA 2013-2017 and Mother Health Care Handbook at Health Care Facilities," 2013, [Online], Available: <http://www.depkes.go.id/article/view/2417/menkesluncurkan-ran-ppaki-2013-2015-ran-ppia-2013-2017-dan-buku-saku-pelayanankesehatan-ibu-di-fas.html>.
- [3] Hartanto W., "Indonesian Maternal Mortality Rate the highest in ASEAN," National Population and Family Planning Board (BKKBN), 2013, [Online], Available: <http://dk-insufa.info/berita/1298-angka-kematian-ibu-di-indonesia-tertinggi-di-asean>.
- [4] Ministry of Health Republic of Indonesia, *Directorate General of Mother-Child Health and Nutrition Development, Guidelines Integrated Antenatal Care*, Second Ed., 2013.
- [5] Soepardi J., "Human Resources for Health Information System," *Center for Data and Information Ministry of Health, Scientific Meeting IX Medical Informatics PSIK Gunadarma*, Depok-West Java, Indonesia, 2012.
- [6] Hosizah, *et al.*, "Designing Electronic Integrated Antenatal Care (in Bahasa)," *Media Kesehatan Masyarakat Indonesia*, vol. 11, 2015, [Online], Available: <http://journal.unhas.ac.id/index.php/mkmi/article/view/539>.

- [7] Kusyanti, A., and A. K. M. Ma'ruf, "The Role of Privacy Concerns and Trust in User Acceptance of Instant Messaging Usage Intention," *International Journal of Computer Science and Information Security*, vol. 14, no. 12, pp. 584–88, 2016.
- [8] Sun, Y., N. Wang, X. Guo, and Z. Peng, "Understanding the Acceptance of Mobile Health Services: A Comparison and Integration of Alternative Models," *Journal of Electronic Commerce Research*, vol. 14, no. 2, pp. 183–200, 2013.
- [9] Russo R., "Best Practice in Health Records Documentation," in Fahrenholz C. G. and Russso R., *Documentation Health Records, American Health Information Management Association (AHIMA)*, Chicago Illinois, pp. 396-429, 2013.
- [10] Cilliers L., Flowerday, S.V., "Health information systems to improve health care: A telemedicine case study," *SA Journal of Information Management*, vol. 15, pp. 1, 2013.
- [11] Kendal K. E. and Kendal J. E., *Design and Analysis System*, Eight Ed., New Jersey, Pearson Education Asia Pte Ltd., pp. 31-42, 2011.
- [12] Lazar, J., J. H. Feng, and H. Hochheiser, *Research Methods in Human-Computer Interaction*, Chichester, UK: Wiley, pp. 206–13, 2010.
- [13] Forrestal, E., "Research Methods," In P. K. Oachs and A. L. Watters (Editors), *Health Information Management: Concepts, Principles, and Practice. 5th ed. Chicago, IL: American Health Information Management Association*, pp. 563–606, 2016.
- [14] R. Akrouf, "Vulnerability analysis and evaluation of intrusion detection systems for Web applications," 2012.
- [15] Pandya D., Patel NJ., "OWASP Top 10 Vulnerability Analyses in Government Websites," *International Journal of Enterprise Computing and Business Systems*, vol. 6, no. 1, 2016.
- [16] Sedek KH, et.al, "Developing a Secure Web Application Using OWASP Guidelines," *Computer and Information Science*, vol. 2, no. 4, 2009.
- [17] Rao KRM, Pant D., "Security risk assessment of Geospatial Weather Information System (GWIS): An OWASP based approach," *International Journal of Computer Science and Information Security*, vol. 8, no. 5, Aug. 2010.
- [18] https://www.owasp.org/index.php/Main_Page.
- [19] World Health Organization (WHO), "Management of Patient Information: Trends and Challenges in Member States: based on the findings of the second global survey on eHealth," *Global Observatory for eHealth Series*, vol. 6, 2012.
- [20] Trimmer, K., L. W. Cellucci, C. Wiggins, and W. Woodhouse, "Electronic Medical Records: TAM, UTAUT and Culture," *International Journal of Healthcare Information Systems and Informatics*, vol. 4, no. 3, pp. 55–68, 2009.
- [21] United States Department for Health and Human Services, "Electronic medical records," The Office of the National Coordinator for Health Information Technology, US Department for HHS, 2012, [Online], Available: http://healthit.hhs.gov/portal/server.pt/community/electronic_medical_records/1219/home/15591.
- [22] Amatayakul, M. A., "Health Information Systems Strategic Planning," In P. K. Oachs and A. L. Watters (Editors), *Health Information Management: Concepts, Principles, and Practice. 5th ed. Chicago, IL: American Health Information Management Association*, pp. 385–421, 2016.
- [23] Johnson, D. L., and C. M. Spielman, "Data and Information Management," In K. M. LaTour and S. E. Maki (Editors), *Health Information Management: Concepts, Principles and Practice. 3rd ed. Chicago, IL: American Health Information Management Association*, 2010, 111–42.
- [24] Kijisanayotin, B., S. Pannarunothai, and S. M. Speedie, "Factors Influencing Health Information Technology Adoption in Thailand's Community Health Centers (CHCs): Applying the UTAUT Model," *International Journal of Medical Informatics*, vol. 78, pp. 404–16, 2009.
- [25] Van Houwelingen, C. T. M., A. Barakat, R. Best, W. R. Boot, N. Charness, and H. S. M. Kort, "Dutch Nurses' Willingness to Use Home Telehealth," *Journal of Gerontological Nursing*, vol. 41, no. 4, pp. 47–56, 2015.
- [26] Rochjati P., *Screening of Risk Pregnancy Poedji Rochjati Method*, Surabaya, Indonesia: Airlangga Press, 2002, pp. 65–73.
- [27] World Health Organization (WHO), "International Statistical Classification of Diseases and Related Health Problems-Tenth Revision," Geneva, 2010.