Gyancity Journal of Electronics and Computer Science,
Vol.5, No.1, pp. 56-75, March 2020
ISSN: 2446-2918 DOI: 10.21058/gjecs.2020.51007

Owasp Approach to Secure Authentication of Online Child Registration

Danilo Alberto Chávez Espíritu

National Registry of Identification and Civil Status-RENIEC
chavez.danilo@gmail.com

Abstract

The objective of this research is to securely authenticate online registration of minors in the Nominee Register as a contribution to reducing the social gap in early childhood, considering that the information provided by RENIEC is information that must have high levels of security, which however should not be an obstacle to access from any place more distant places where the Government should have a presence, in this sense the OWASP (Open Web Application Security Project), open project, which is referenced by many standards of security, as a result of this implementation it was possible to securely authenticate online registration, significantly reducing vulnerabilities in all application phases, which has enabled strategic alliances with MEF and MINSA to bring technology safely to the different parts of Peru where there was little presence of the State which has allowed in the Nominal Register with the registration of children from early childhood to reduce the social gap in relation to inclusion.

Keywords: OWASP, Web technology, Nominal Register, Security, Social gap

I. INTRODUCTION

There are many children in early childhood from zero to five years, which the State does not reach due to various limitations, despite the various inclusion programs, this research seeks to indirectly reduce the social gap of these minors by applying web technology secure and the registration and identification in a Nominee Register that must fully attend to these minors to remove them from a risky situation. Hence, it is crucial to collect all the information that allows correcting the lack of real data,

indicators and statistics and timely about the various risks to the health of young children, as well as education that requires the intervention of the State. The lack of monitoring and traceability of the infant's real situation does not allow evaluating the fulfillment of goals, the evolution, and evaluation of the progress made in favor of children. On the other hand, the non-implementation of secure technologies related to identification, prevent the correction of errors of unavailability of information, which hinders the possibility of improving the situation faced by minors in early childhood, the absence of identification, not It allows to have indicators of access to health care. So the research question is: How is it possible to securely authenticate the online registration of early childhood minors in the Nominated Register as a contribution to reducing the social gap? So the general objective: is Securely validate the online registration of children in the Nominated Register as a contribution to reducing the gap. There are many children under the age of five included in early childhood, who are chronically malnourished, who must be adequately addressed by the State to remove them from a risky situation, so it is important to collect all the information to correct not having real and timely data, indicators and statistics about the various risks to the health of young children, as well as education that require state intervention. The lack of monitoring and traceability of the infant's real situation does not allow evaluating the fulfillment of goals, the evolution, and evaluation of the progress made in favor of children. On the other hand, the non-implementation of secure technologies related to identification, prevent the correction of errors of unavailability of information, which hinders the possibility of improving the situation faced by early childhood children, the absence of identification does not allow to have indicators of access to health care. The RENIEC is the entity responsible for registering and identifying all Peruvians and issuing the national document that accredits it; the MINSA is responsible for keeping a record called the Nominal Register that must contain the data of minors up to 6 years that require to be cared for in the medical centers, hospitals and medical posts nationwide that are mainly vaccinated (Ministerial Resolution 070-2011) and for this it is necessary to know if the minors are registered if they have a DNI or not. By logging in the Nominated Register, it is expected to identify documented and undocumented persons.

II. Theoretical framework

According to Ñique (2016), technology presents new environments. Still, they also expose us to risks such as identity theft, because they lack robustness when authenticating, making it easier for these unprotected organizations to be violated, and it is necessary to implement protection systems that consider alternatives for double factor authentication. Urquizo (2016), for his part, identifies those factors that

critically affect the adequate registration, in this way he proposes to apply awareness programs that reduce errors when registering citizens, the research also addresses the importance of considering the sociocultural characteristics of the People who register to provide a methodology that considers what is necessary to ensure their learning, this research also seeks to identify the potential of the registrar to improve service to citizens. According to Lay (2015), the new theories of childhood sociology, in their participation builds childhood according to the image that adult children have, the methodology used is framed an interpretative orientation, in an approach that characterizes addressing the assistance of the infant in an inclusive way that adds experimental elements and knowledge of the adult environment as guiding principles related to social organization that seeks to include and integrate the infant with a methodology that allows establishing actions with a comprehensive vision to promote a collaborative approach trying to achieve childhood well-being.

III. Conceptual definitions

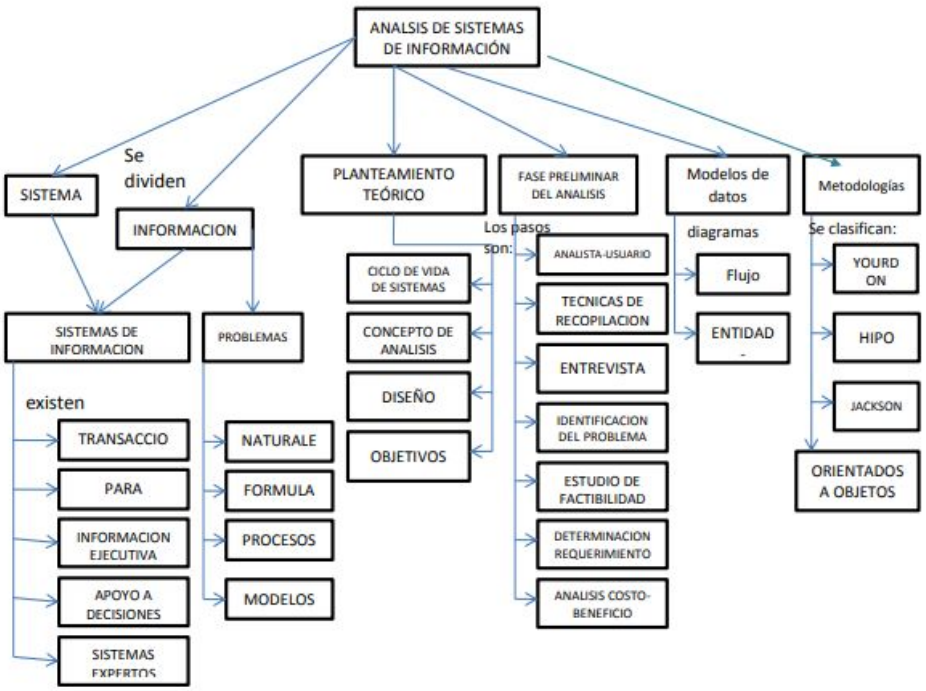


Figure 1: Information Systems Source: Luis Antonio Dominguez Coutiño 2008

3.1 General Systems Theory

According to Dominguez (2012), "The general theory of systems has its origin in the works carried out by the German biologist Von Bertalanffy, released publicly between 1950 and 1968". This theory, in turn, generates conceptual formulations to be applied empirically in the analysis of information systems, Figure 1.

This theory allows us to:
• Integrate various knowledge.
• Orient a single theory.
• Develop other areas of scientific knowledge.
• Approaching scientific research objectives of contributing to knowledge and society.

The General Systems Theory in its understanding of systems is manifested in the general analysis, considering the relationships of systems in relation to:

3.2 Social Identity

Scandroglio, López, & San José (2008) explain that the "Theory of Social Identity (TIS) and the Theory of Self-Categorization of the Ego have had a great influence on contemporary Social Psychology, providing notable contributions to the understanding of the social dimension of behavior." The research reviews the components of Social Identity Theory. It explains the efforts of works and interpretations that explain group behavior considering the dimensions, context, and identification processes to analyze group events in a manner consistent with their complexity.

3.3 Network security:

Klooster (2016), in his research on "Application of a security testing methodology: a case study," explains that security testing is a discipline of software testing that aims to verify whether it is protected and the resistance of its functionality against attacks on it and on processed data. Security standards are published to establish common requirements that the software must meet. This research describes and applies a process necessary to verify the security of a web application using a security requirements checklist that combines the OWASP ASVS and OWASP Top Ten Project web application security standard. Test cases were developed, and the UXP Portal web application was tested to verify the security requirements in the checklist, numerous security vulnerabilities were identified, identified by security tests as well as recommendations based on the lessons learned during the study of the case presented.

3.4 Security on the Web

According to Corona (2010), computer security addresses the weaknesses of information processing, considering that currently, the Internet is the primary vector in the processing and exchange of information, and web-based architecture represents the standard for accessing data. Internet services. It is proven that the weakness of security is through the Internet and is in: users who browse the Web and web applications on the server-side that process information, the research presents two approaches to security systems, which They contribute significantly to the security of web browsers and to applications on web servers that are typical "weak points.". Thulin (2015), in his proposal of "Evaluation of the applicability of security testing techniques in continuous integration environments," explains that agile development methodologies are increasingly popular, especially in projects that develop web applications. However, incorporating software security into light approaches can be difficult. Using security testing techniques throughout a complete agile development process running automated tests in continuous integration environments is an approach that strives to improve security in agile projects. Instead of conducting security tests at the end of the development cycle, these methods allow early and continuous detection of security risks and vulnerabilities. Singh Bisht (2011) in his research on improving web security by automated extraction of web application intent, explains that over the past decade, the Web has been transformed into a sophisticated and distributed computing platform, primarily enabled by applications web as evidenced by the success of sites like Facebook and YouTube. The objective is to investigate fundamental ways to improve the security of existing web applications, with research efforts in two complementary directions: a) techniques to discover security flaws and b) techniques to automatically correct security flaws.

3.5 Social gap

A social gap is considered to be the separation, opening or distance with society, the community and the people who interact with each other sharing the same culture, the gap is a crack in society, a social gap is a form of inequality where the group of people does not have possibilities of access to the benefits of the State, which requires improving the conditions of those not included in search of a social balance, the indicators of measurement of the social gap can be calculated by the level of income, education, quality of employment, housing, services, access to health and social programs, reducing a social gap contributes to improving the dignity of the human being and being part of the inclusion of the State (Pérez Porto, 2016).

3.6 Web Technology

It is the technology that allows access to resources available on the Internet through a browser to facilitate access to data and information as well as developments that manage knowledge, due to its flexibility, ease of use and deployment.

IV. Methodology

According to the purpose, it starts from the identification of the problem, its nature, the objectives of the research and the work proposal that brings together methodological conditions to consider it "applied" research, considering that its implementation uses knowledge related to Information Technologies, which is applied in identification records in Peru; It is also a quantitative investigation because it will process real data on the risks of technology, as well as data on minors in early childhood.

4.1 Operationalization of variables

Operationalization is carried out considering the independent and dependent variables, their conceptual and operational definitions, their dimensions, indicators, and instruments, according to Table 1.

Table 1 Operacionalización de variables

	Variable	Conceptual definition	Operational definition	**Dimensions**	**Indicators**	**Instruments**
Independient Variab	Early childhood children	An individual whose age is between "0" and "5" years includes the minority of age and all childhood.	Considers children in early childhood who have not had access to state services as part of the social gap of the excluded	Levels of 0 to 1 Levels of 1 to 2 Levels of 2 to 3 Levels of 3 to 4 Levels of 4 to 5	A number of unidentified children. Origin of children Children's language Parents conditions	Interviews
	Web Technology Risks	Probability of an event that impacts the application of technology	The materialization of the threat that may violate web systems that contain sensitive information from citizens	Risks Web Technology	Probability Impact.	OWASP framework

le						
Dependent Variable	Social gap	Separation, openness or distance in the social community and people who interact with each other sharing the same culture, is a social rift	Desigualdad social que afecta a la inclusión de los menores de edad en su participación de los programas en los cuales el Estado busca ampliar para el acceso a la salud y educación como parte de la inclusión.	Health care gap Education gap Inclusion gap	-Literacy level. -Access to public services. -Participation in social programs	Register of Indicators in the Nominal Register

4.2 Population and sample

It is considered minors of early childhood who live in a certain jurisdictional area of a district of Peru, where it is expected to close gaps in access to identification, a necessary condition for access to citizen rights and State interventions in health, education, food as a sector objective related to the reduction of malnutrition in the infant population of early childhood children, to monitor. The sample is the portion of minor children from early childhood that represents the population, who will be registered and registered in the Nominated Register in the municipalities and districts of the regions of Peru, initially in Amazonas, Huánuco, and Cajamarca, and later extend to the other registry offices to which it is intended to provide identification to access their rights in health, education, and food as a sector objective related to the reduction of malnutrition in the infant population of early childhood children, to tracing.

4.3 Data collection techniques and instruments

The main ones that will be considered are:

• Interviews (People)
• Documentary analysis (Documents)

The documentary review will be used to acquire data from primary and secondary sources to help clarify and increase the knowledge of newspapers, reports, and research papers.

• Open source and Denial of Service tools were also used.

4.4 Interview guide

The technique to collect information, a good interview will be to plan said interview properly. The interviewer will be endorsed by an institutional letter that introduced him and explicitly stated the purposes of the interview, affirming his reserved character. An appointment will be made. Previously, approaching the interviewee and the date on which the interview will take place will be coordinated. The interviewer will be able to overcome the difficulties of said interview, as he also had the following qualities: ability to communicate and position himself objectively in the position of the interviewee.

4.5 Instruments for Web

• Agile load for stress and load tests in web applications,
• SoapUI to test the web services and monitor their actions
• Selenium and XPATH are also tools to test the functionality and security of the Web.

4.6 Data processing and analysis

In the processing, data collection is carried out from the instruments established in the operational matrix of variables, which will then be established in a matrix of indicators that will reflect the reasons for evaluating the risks and promote social programs for the reduction of the social gap.

V. Web technology with OWASP approach

This research seeks to apply the OWASP approach (Open Project on Web Application Security) on the Web technology platform and backup, under established security standards and criteria. Secure online registration authentication.

5.1 Test Environment

Infrastructure tests that include Software and Hardware tests are considered. For the software tests were used:

- Windows Operating System
- Internet Explorer in versions 9, 10
- Mozilla Firefox version 39+
- Google Chrome version 43+

For the hardware tests were used: Personal computers with the following minimum characteristics:

- Processor: Intel Pentium IV
- RAM: greater than 512 MB.

In Figure, Nº 2 shows the initial procedure of how the information was managed and supplied in the nominal Register. In the process flow, Excel was used to collect the data and transmit it through the system. In the municipalities, children of early childhood were registered, their passage was through the systems without security measures to MINSA, and they reported to the MEF to evaluate the investment and monitor the project, all with the information provided by RENIEC.

Figure 2 (a): Initial and current procedure of the nominal Register and sending of information.

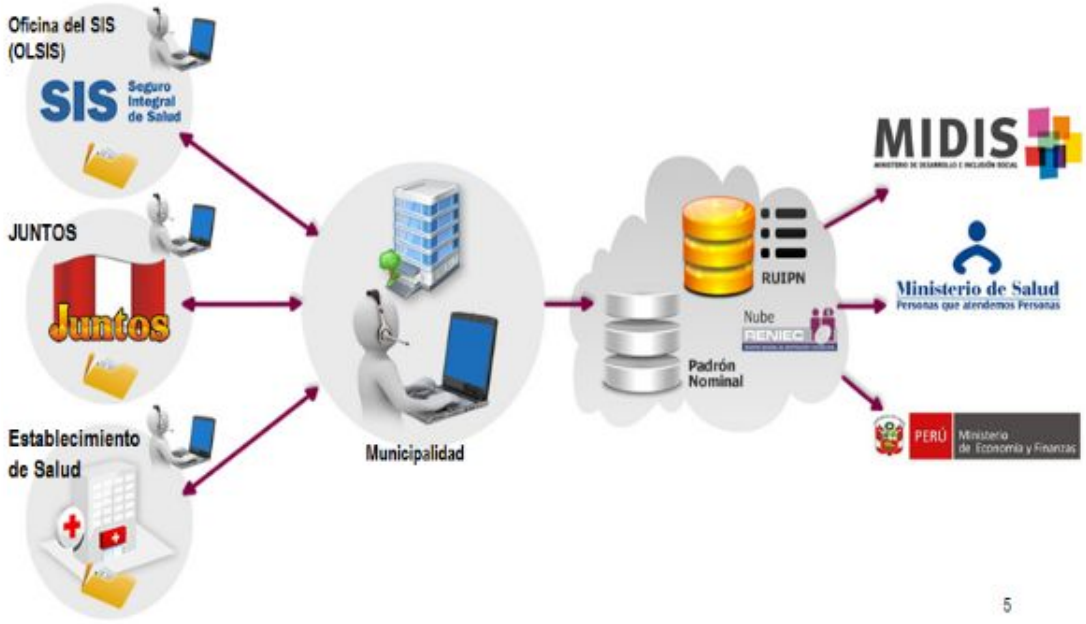


Figure 2 (b): Initial and current procedure of the nominal Register and sending of information.

Figure 2 shows the model of the new communication structure applying Web technology with an OWASP focus, here social programs are integrated and authenticated online registration is carried out in the municipalities; centralized information can be accessed and processed with the respective indicators for decision-making in MIDIS, MINSA and MEF, promoting the arrival of the State to the different sectors not included where the children of early childhood are found.

5.2 Social monitoring with the Nominal Register

The implementation of an authenticated nominal register of early childhood children in the nominated Register is aimed at standardizing and updating the information of children living in a specific jurisdictional area of a district, in this way the Register provides the opportunity to reduce the distance for Obtain the identification, necessary condition of the citizen's right and state intervention, in health, education, food, among others, that converges with the sector objective related to reducing child malnutrition, the results of the Articulated Nutritional Program - PAN are measured in the population of early childhood children, and the Nominal pattern should also contribute to monitoring initial education coverage, which is considerably less than primary education coverage, which is close to 100%.

Gyancity Journal of Electronics and Computer Science,
Vol.5, No.1, pp. 56-75, March 2020
ISSN: 2446-2918 DOI: 10.21058/gjecs.2020.51007

5.3 Development of the application:

The communication interface will be developed to access the registry data as appropriate. The solution must consider that the authorized personnel of the respective municipality is solely responsible for the registration. You must allow any change or alteration of the same to be saved, to be presented before possible audits. The solution validation Pilot test report: validation operations that allow concluding on the functionality and access to the application from the district municipality and the procedure for using and consulting data. The activity includes:

• Preloading the data in the Nominal Register based on the information provided and managed by MINSA.

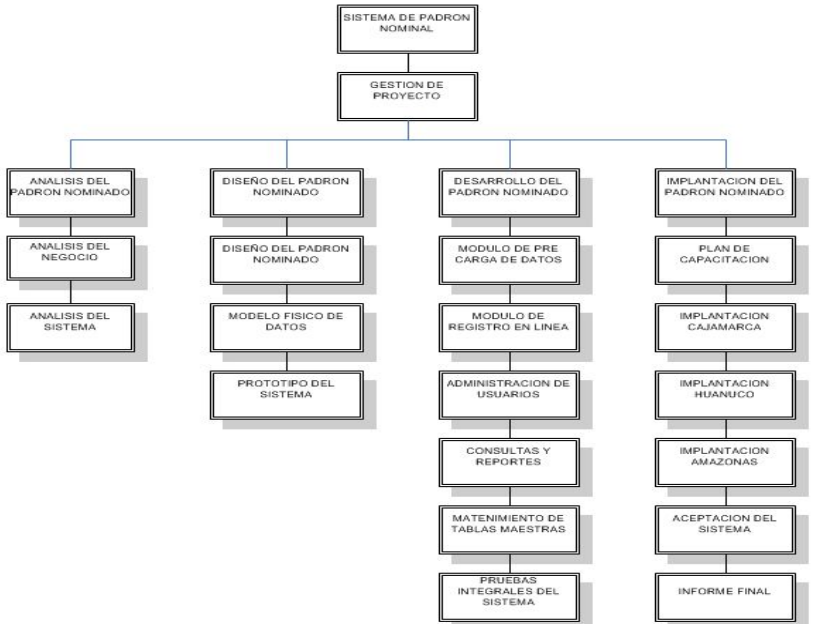


Figure 3 Structure of the Work Breakdown - EDT of the Nominal Register

• Documentation on the validation tests of the application in Margos and Panao districts in the Department of Huánuco, within the framework of the implementation of the articulation of budget programs, focused on early childhood. The tests will be carried out in the same municipality after coordination with authorized personnel (agreeing dates, local contacts, induction modality.

- Identificación de las principales dificultades en la operatividad del sistema de acuerdo a la EDT según la Figura 4.

5.4 Implementation of the Nominal register

The work methodology includes the selection of districts, these districts belong to the first quintile of regional poverty in the regions of Amazonas, Cajamarca, and Huánuco and are the scope of intervention of the JUNTOS program, they are subject to measurement and monitoring according to budget support agreements between the respective regional governments, MIDIS and RENIEC with the MEF. Intersectoral coordination was essential, RENIEC defined the coordination items with the OGEI of MINSA, the fields to be registered in the register and their respective format, access to information on the sectors involved, the reporting formats that the system for different users, the municipalities of selected districts, the method or protocol of the use of the register.

5.5 Homologation and update of the register

To standardize the pattern data, the different sources of information from which the data comes must be compared, and validation criteria must be reviewed to record duly accredited information. The update of the register is carried out as indicated in the instructions for the goal: District nominal register of early childhood children approved and updated, to update the register, monthly meetings will be held between the municipal manager of the nominal register and his representatives from the respective local instances. As a result of the meetings, an act is prepared and signed, describing the agreements made and the progress that has been made to complete the data of the nominal register. RENIEC preloads data from different information providers such as health facilities, the Juntos program, the Municipal Registry Office, the SIS, the Ministry of Education, the glass of milk program, among others. For this, the sources of information with which the preload is carried out are identified (at which level said the report is produced and how it is consolidated at the district level). According to the establishments, the information provided by the health establishment of the district capital or higher resolution category in the district scope is taken into account.

VI. Results

The tests carried out were as follows:

For all cases, the following scheme was developed as shown in Figure 5.

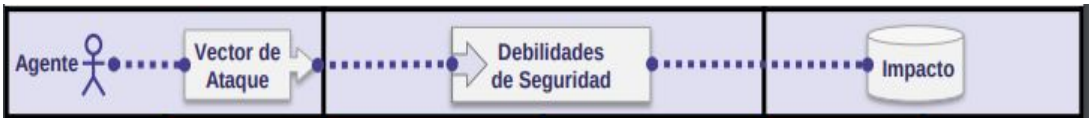


Figure 4 Scheme Attack-Impact Source: OWASP top 10

6.1 Injection:

Injection to SQL, NoSQL, OS or LDAP, is presented as part of a query when the interpreter receives or sends unreliable data, this data can or deceive the interpreter by inducing the execution of commands to access the data without the due authorization. Its exploitability (3) from a specific application from any source such as variables, parameters, internal and external web services, and to any user.

6.2 Loss of Authentication

When authentication and session management are not properly implemented, then there is an opportunity for attackers to compromise users, passwords, implementation as well as to impersonate identity. Its exploitability (2) from a specific application occurs when attackers have access to the user, password, and default combinations to administrative accounts, from where they carry out brute-force or dictionary attacks.

6.3 Exposure of sensitive data

Web applications and APIs are not exempt from being violated to expose data such as financial, health, or personal information. Theft or modification of data not adequately protected facilitates, fraud or the crime is not an opportunity.
Its exploitability (2) from a specific application instead of attacking crypto, attackers steal keys, execute "man in the middle" attacks or steal data from the server, or the client. A manual attack is required, but databases with hashes that have been made public can be used to obtain the original passwords using GPUs.

6.4 External XML Entities (XXE)

Old or poorly configured XML processors evaluate entity references in XML documents. Entities can be used to reveal internal or internal files on outdated servers, scan LAN ports, remotely execute code, and perform denial attacks.
Its exploitability (2) from an application in which attackers can exploit vulnerable XML processors if they load or include hostile content in an XML document, using sensitive code, dependencies, or integrations.

6.5: Loss of access control

Failure to apply the restrictions established to authenticated users can cause attackers to exploit vulnerabilities to gain unauthorized access to functionality, data, accounts, files, and may change access rights and permissions.
Its exploitability (2) from an application is the exploitation of control access, is an essential skill of attackers. The SAST and DAST tools can detect the absence of access controls but, if they are present, they cannot verify if they are correct. It is detectable using manual means or automatically in some frameworks that lack access controls.

6.6: Incorrect Security Configuration)

This is a widespread problem and is due in part to set the configuration manually, ad hoc, or by default (or directly due to lack of configuration). Examples are S3 open buckets, poorly configured HTTP headers, error messages with sensitive content, lack of patches and updates, frameworks, outdated components, and dependencies, etc.
Its exploitability (3) from an application (2) where attackers will often try to exploit vulnerabilities without patching or accessing default accounts, unused pages, files, unprotected directories, to access the system or the business.

6.7: Cross-Site Scripting (XSS)

They occur when unreliable data is entered and sent to the web without validation and proper coding, or the existing website is updated with user-supplied data with an API that runs scripts in the browser. They allow you to execute commands to hijack a session, perform a defacement on the web, or redirect. In the exploitability (3) of a specific application, there are automated tools to detect and exploit the three forms of XSS, and free exploit kits are also available.

6.8: Insecure Deserialization

These defects occur when an application receives harmful serialized objects, and these objects can be manipulated or deleted by the attacker to perform replay attacks, injections, or elevate their execution privileges. In the worst-case scenario, insecure deserialization can lead to remote code execution on the server.
In the exploitability of a specific application, the aim is to achieve the exploitation of deserialization that is difficult, since distributed exploits rarely work without changes or adjustments in their source code.

6.9: Use of components with known vulnerabilities

Components run with privileges assigned in the application. If an element is breached, the attack will take data or control of the server. Therefore application vulnerabilities and APIs will weaken application defenses with various attacks and impacts.
Exploitability It is easy to obtain exploits for already known vulnerabilities, but the exploitation of others requires considerable effort, for their development and customization.

6.10: Insufficient Registration and Monitoring

It is the lack of response to attacks that can occur over time and that try to manipulate, extract or destroy data. The exploitability (2) of the specific application shows insufficient recording and monitoring is the basis of almost all significant and major security incidents. Attackers depend on a lack of monitoring and timely response to achieve their goals without being detected. The following Figure 5 summarizes the results of the vulnerability test cases with the OWASP application as evaluated in a development and testing environment.

Nivel de riesgo	Número de alertas	Color según nivel
Alto Riesgos con probabilidad de ocurrencia alta	13	Rojo
Medio Riesgos con probabilidad de ocurrencia media	8	Naranja
Bajo Riesgos con probabilidad de ocurrencia baja	2	Amarillo
Informativo	0	-

Figure 5 Test case SQL injection failure: A1 Injection Source: Own elaboration

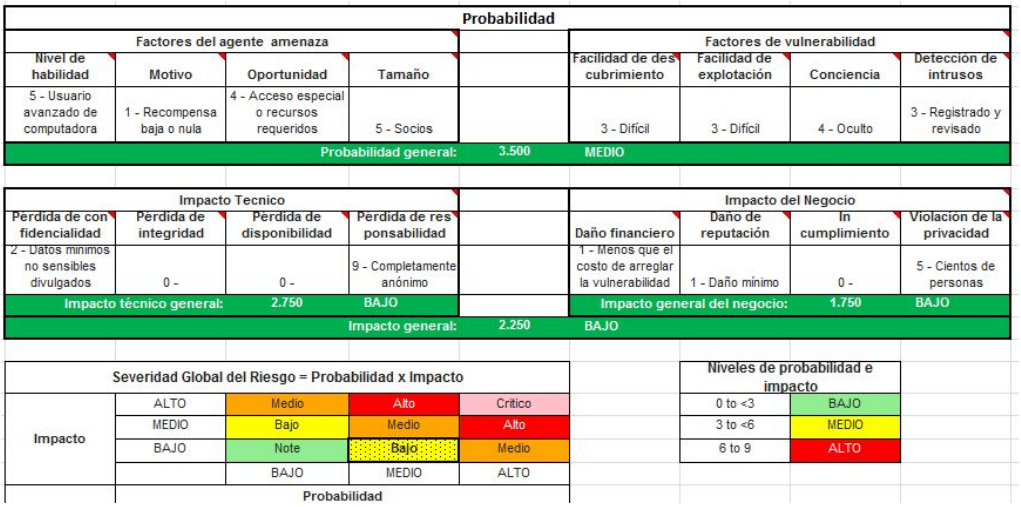
The compromised URLs that were identified and subjected to the corresponding tests were:
http://weblogdev7.reniec.gob.pe:7001/padronn/registromanual/buscarmenor.do?dni=63439104
http://weblogdev7.reniec.gob.pe:7001/padronn/registromanual/formulario.do?coPadronNominal=81243825&_=1442876678835
http://weblogdev7.reniec.gob.pe:7001/padronn/registromanual/guardar.do

From the results obtained, it was identified that there is no confidence in the client's entry data, requiring.
• Check the login data to the server.
• Identify the use of JDBC, and if so, use the PreparedStatement, CallableStatement methods with parameters passed by '?'
• It is preferable to use stored procedures on the BD.
• Strings must not be concatenated strings in queries and stored procedures.
• Use run or run immediately or equivalent functionality.
• Avoid creating weak string concatenation in dynamic SQL queries.
• Consider a white list or blacklist of allowed characters and not on the user input side.
• Implement privilege control with restrictions and necessary for DB users.
• Minimize the impact of SQL injection by preventing DB users from using 'sa' or 'DB-owner.

Caso de Prueba:	CP_003: X-Frame-Options No Set Header				
Requisitos:	El aplicativo no debe permitir ataques de tipo 'ClickJacking', del lado del cliente y del lado del servidor.				
Propósito de Prueba:	Los datos de RENIEC deben permanecer inalterables y seguros.				
Naturaleza de la prueba:	Positiva				
Modo de prueba:	Sistemático				
Pre-Condiciones:	Usuario registrado, activo y logueado en el sistema.				
Datos de entrada:	• Usuario:				
Descripción de la prueba:	1. Acceder al sistema 2. Ingresar un modulo 3. Ingresar al software OWASP ZAP 4. Aplicar un Escaneo Activo (Nivel Alto) 5. Analizar las Alertas mostradas				
Criterios de éxito	Los pasos se han ejecutado correctamente.				
Post- condiciones:					
Fecha	**Encargado**	**Pruebas**	**Riesgos hallados**	**Nivel de riesgo**	**Comentario**
		1	1	Medio	La cabecera X-Frame-Options no está incluida en la respuesta HTTP para proteger contra ataques 'ClickJacking'.

Gyancity Journal of Electronics and Computer Science,
Vol.5, No.1, pp. 56-75, March 2020
ISSN: 2446-2918 DOI: 10.21058/gjecs.2020.51007

Figura 6 CP_003:X-Frame-Opcions No Set Header : A3 Exposición de datos



Probabilidad								
Factores del agente amenaza					Factores de vulnerabilidad			
Nivel de habilidad	Motivo	Oportunidad	Tamaño		Facilidad de descubrimiento	Facilidad de explotación	Conciencia	Detección de intrusos
5 - Usuario avanzado de computadora	1 - Recompensa baja o nula	4 - Acceso especial o recursos requeridos	5 - Socios		3 - Difícil	3 - Difícil	4 - Oculto	3 - Registrado y revisado
Probabilidad general:				3.500	MEDIO			

Impacto Tecnico					Impacto del Negocio			
Pérdida de confidencialidad	Pérdida de integridad	Pérdida de disponibilidad	Pérdida de responsabilidad		Daño financiero	Daño de reputación	Incumplimiento	Violación de la privacidad
2 - Datos mínimos no sensibles divulgados	0 -	0 -	9 - Completamente anónimo		1 - Menos que el costo de arreglar la vulnerabilidad	1 - Daño mínimo	0 -	5 - Cientos de personas
Impacto técnico general:		2.750	BAJO		Impacto general del negocio:		1.750	BAJO
Impacto general:				2.250	BAJO			

Severidad Global del Riesgo = Probabilidad x Impacto				
Impacto	ALTO	Medio	Alto	Critico
	MEDIO	Bajo	Medio	Alto
	BAJO	Note	Bajo	Medio
		BAJO	MEDIO	ALTO
	Probabilidad			

Niveles de probabilidad e impacto	
0 to <3	BAJO
3 to <6	MEDIO
6 to 9	ALTO

Figure 7 Risk Level Matrix

In Figure 7, the risk level matrix shows the number of alerts with a high probability of occurrence. The identified alerts are evaluated in the probability and impact matrix.

Table 2 Calculation of probability and impact for risks according to OWASP

Table *Paired Sample Statistics*

	Mean	N	Standard deviation	Mean standard error
Pos test	1,6700	10	0,95581	0,30225
Pre test	7,5070	10	2,13767	0,67599

6.11 Hypothesis testing

According to the data processing carried out, regarding the null hypothesis, it is necessary to:
H1: There is a difference between the Pretest without OWASP and the Post-test with OWASP, the hypothesis is accepted.
The level of significance was considered 5%
The normality of the pretest and post-test variables was checked

Test Statistic
T-student for related or paired samples

Table 3: Test for paired sample statistics

	Paired differences					t	gl	Sig. (bilateral)
	Mean	standar Deviatión	Media de error estándar	95% confidence interval of the difference Lower	Upper			
Pos test – Pre test	-5,837	2,64302	0,83580	-7,72771	-3,94629	-6,984	9	0,000

Decision: p-value = 0.000 <0.05 hypothesis H0 is rejected
Conclusion: There is a significant difference between the Pretest without OWASP and the Post test with OWASP, with a significance level of 0.05

Table 4: Goals of the Municipal Incentive Plan. Source: RENIEC website

Test of Kolmogorov-Smirnov one sample

		Pretest	Postest
N		10	10
Parámetros normales	Mean	7,5070	1,6700
	Stándar Deviatión	2,13767	,95581
Máximas diferencias extremas	Absoluta	,147	,155
	Positive	,147	,155
	Negative	-,145	-,135
Estadístico de prueba		,147	,155
Sig. asintótica (bilateral)		**0,200**	**0,200**

Percentage of early childhood children benefiting from the Together Program. For the dependent variable, we have the indicators that record the reduction of the social gap. Early childhood children who have a DNI by origin.

Gyancity Journal of Electronics and Computer Science,
Vol.5, No.1, pp. 56-75, March 2020
ISSN: 2446-2918 DOI: 10.21058/gjecs.2020.51007

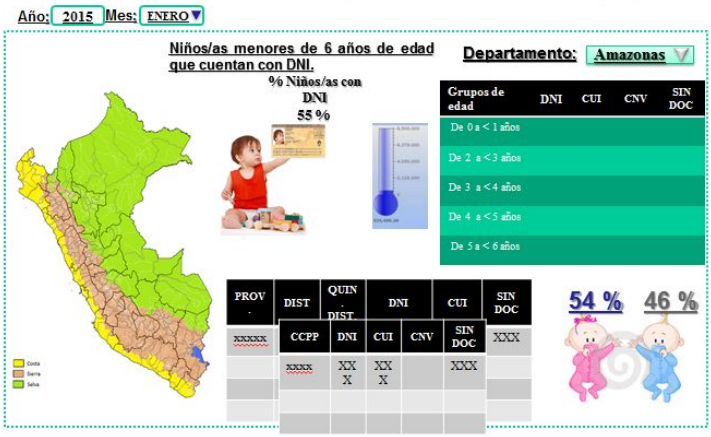


Figure8: Nominal Register Indicators

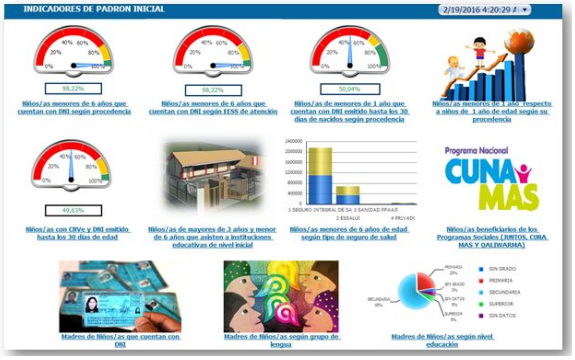


Figure 9 (a): Goals of the Municipal Incentive Plan. Source: RENIEC website

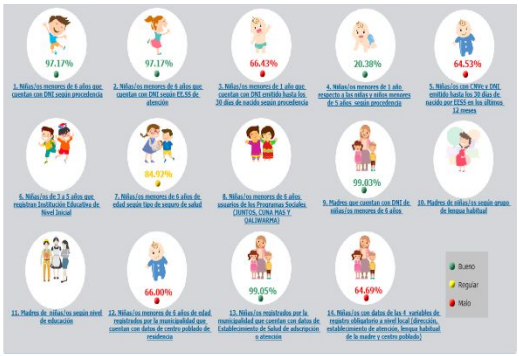


Figure 9 (b): Goals of the Municipal Incentive Plan. Source: RENIEC website

The reduction of the social gap is shown with the levels of the indicators of access to services for young children in early childhood, which has been made possible by monitoring and decision-making with the application of the programs.

7. Conclusion

The objective of securely authenticating the online registration of early childhood minors in the Nominated Register was achieved, as well as the hypothesis that the implementation of web technology with an OWASP approach allows authentication, which means accrediting, securing and certifying. the integrity of the data to be processed in the transactions and the online registration of early childhood minors of the Nominee Register is carried out safely, having reduced the risks with the 10 OWASP standards from a high level to a low level, allowing to reach with technology web to the most remote registry offices providing indicators to reduce the social gap and minimize the risk of online registration of early childhood minors in the Nominated Register

References

Avella Villamil, A. M. (2015). ¿QUE EFICACIA HA TENIDO LA POLÍTICA PÚBLICA COLOMBIANA DE PRIMERA INFANCIA "DE CERO A SIEMPRE"? Tesis, UNIVERSIDAD MILITAR NUEVA GRANADA, RELACIONES INTERNACIONALES Y ESTUDIOS POLÍTICOS, Bogotá. Colombia.

Corona, I. (2010). *Deteccion de ataques a la Web.* Universidad de Cagliari, Departamento de Ingenieria Electrica y Electronica. Cagliari: Universidad de Cagliari.

Dominguez, L. A. (2012). *Análisis de Sistemas de Información* (Primera ed.). (R. T. MILENIO, Ed.) Tlalnepantla: RED TERCER MILENIO. doi:978-607-733-105-6

Klooster, K. (2016). *Applying a Security Testing Methodology: a Case Study.* UNIVERSITY OF TARTU, Institute of Computer Science. Tartu: UNIVERSITY OF TARTU.

Lay Lisboa, S. L. (2015). *LA PARTICIPACIÓN DE LA INFANCIA DESDE LA INFANCIA La Construcción de la Participación Infantil a Partir del Análisis de los Discursos de Niños y Niñas.* Tesis Doctoral, Universidad de Universidad de Valladolid, Facultad de Educación y Trabajo Social Departamento de Pedagogía, Segovia, España.

MINSA. (2018). *Ministerio de Salud.* Recuperado el 14 de Enero de 2018, de http://www.minsa.gob.pe/portalweb/02estadistica/estadistica_26.asp

Ñique Morazzani, V. A. (2016). *IMPLEMENTACIÓN DE SOLUCIÓN DE AUTENTICACIÓN SEGURA BASADA EN DOBLE FACTOR EN UNA ENTIDAD DEL ESTADO.* Tesis, Universidad San Ignacio de Loyola, FACULTAD DE INGENIERÍA, Carrera de Ingeniería Informática y de Sistemas, Lima, Perú.

OWASP. (s.f.). Recuperado el 14 de Enero de 2018, de https://www.owasp.org/index.php/Proyectos_OWASP

Pérez Capdevila, J. (2018). *Tecnoweb2.* Recuperado el 14 de Enero de 2018, de http://tecnoweb2.com/tecnologias-web

Pérez Porto, J. (2016). *Definicion.* Recuperado el 14 de Enero de 2018, de https://definicion.de/brecha-social/

Scandroglio, B., López, J., & San José, C. (2008). *La Teoría de la Identidad Social: una síntesis crítica de sus fundamentos, evidencias y controversias.* Paper, Universidad Autónoma de Madrid, Madrid. Obtenido de http://www.psicothema.es/pdf/3432.pdf

Singh Bisht, P. P. (2011). *Improving Web Security by Automated Extraction of Web Application Intent.* University of Illinois, Computer Science. Chicago: University of Illinois.

Thornberry, G. (2015). *PALESTRA PORTAL DE ASUNTOS PÚBLICOS DE LA PUCP.* (PUCP, Ed.) Recuperado el 14 de Enero de 2018, de http://repositorio.pucp.edu.pe/index/bitstream/handle/123456789/11954/quien_soy_yo_Thornberry.pdf?sequence=1

Thulin, P. (2015). *Evaluation of the applicability of security testing.* Linköpings universitet, Department of Computer and Information Science. Linköping: Institutionen för datavetenskap.

Urquizo Limache, G. R. (2016). *La capacitación de los registradores civiles impartida por el Registro Nacional de Identificación y Estado Civil (RENIEC) y su eficiencia en la función registral.* Tesis de magister en Gerencia Social, PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ, ESCUELA DE POSGRADO, Lima, Perú.