Vol 8. No. 3 Issue 2 – October, 2015

African Journal of Computing & ICT

www.ajocict.net

A Survey of Security Vulnerabilities in PHP Applications among IT Professionals in Nigeria

O. Oyemade & J.O. Odiagbe
Research Student, M.Sc. Information Technology
National Open University of Nigeria
Sokoto Study Center – Nigeria
pharmtex08@yahoo.com

B. A. Buhari
Department of Mathematics, Computer Science Unit
Usmanu Danfodiyo University
Sokoto – Nigeria
buhari.bello@udusok.edu.ng

ABSTRACT

This research performs a survey of security vulnerabilities in PHP Application among IT professionals in Nigeria. We targeted 170 IT Professionals in various ICT organizations and institutions in Nigeria. The main instrument for data collection was questionnaire. Stratified random method was used to select respondents from various strata. A total of 170 specialists in the sample which included 95 from ICT organization, 55 from MIS department of higher institutions and 20 ICT lecturers were randomly selected. The data collected from questionnaire were analyzed using simple frequencies and percentages. It was found out that higher numbers of respondent are conversant with PHP and using PHP always, two causes of the security vulnerabilities, SQL injection and source code revelation are been highlighted by the majority of the respondents. Also, majority of respondents were recorded to be having database hacking challenges and suggested that developer should use all the appropriate security measures and function to secure the application i.e. using ESCAPE FUNCTION, Turned OFF register_globals directive etc. PHP is rates high in terms of portability and accessibility, security, ease of operation and comparison to other applications.

Keywords – Security, Security Vulnerabilities, PHP, IT Professional, SQL Injection, PHP Applications

African Journal of Computing & ICT Reference Format:
O. Oyemade, B.A. Buhari & J.O. Odiagbe (2015): A Survey of Security Vulnerabilities in PHP Applications among IT Professionals in Nigeria. Afri J Comp & ICTs Vol 8, No.3 Issue 2 Pp 177-183.

1. INTRODUCTION

Web applications in particular are being used today as front ends to many security critical systems (e.g., home banking and e-commerce), but due to their high exposure, they are particularly susceptible to being heavily attacked or become attractive targets for attackers due to the large degree of authority they possess, their significant user populations, and the prevalence of vulnerabilities they contain.. This means that they require special care to make them secure and resilient against these threats. PHP is one of the two leading development frameworks for these dynamic web sites. It is also the foundation for popular web development applications such as Drupal, Joomla, and Wordpress. Thus the task of securing PHP web applications is urgently needed. In fact, 60% of found vulnerabilities affect web applications [1]. As such, much attention in the security research community has focused on removing or justifying the effect of these vulnerabilities [2], [3], [5], [5] and enhancing the security of these e-commerce and banking systems like security enhanced online registration prepaid scratch payment approach [6].

Security vulnerabilities in these web applications may result in stealing of confidential data, breaking of data integrity or affect web application availability. This research performs a survey of these security vulnerabilities in PHP Application among IT professionals in Nigeria. We target 170 IT Professionals in various ICT organizations and institutions in Nigeria. The main instrument for data collection was questionnaire. These questionnaires were used to enable these IT professionals to highlight causes of security vulnerabilities, security challenges they are facing and strategies they employ in finding solutions to these security vulnerabilities in PHP. Also, to rate the PHP in terms of portability and accessibility, ease of operation, security and comparison to other applications. Stratified random method was used to select respondents from various strata in which there were a total of 170 specialists in the sample which included 95 from ICT organization, 55 from MIS department of higher institutions and 20 ICT lecturers were randomly selected. The data collected from questionnaire were analyzed using simple frequencies and percentages.

2. METHODOLOGY

This study employed descriptive survey research design. It is a method of collecting information by administering a questionnaire to a sample of individuals. Descriptive surveys are designed to obtain information about the current status of a phenomenon or to answer questions like where, what, how, why, when, and who. It is intended to produce statistical information about a research area [7].

2.1 Target Population

Specifying the population that is targeted for study is important because it helps researcher to make decisions on sampling and resources to use [8]. This study targeted 170 IT Professionals in various ICT organizations and institutions in Nigeria. The categories of personnel use is 6 based on their area of specialization in Software Development.

2.2 Sampling Size and Sampling Procedure

Stating the sample size and sampling procedures is important in order to establish representativeness of the sample for generalization [9]. This can be due to various factors that may hinder studying the whole population [10]. Also, sampling procedures are strategies or procedures that are used to select a sample from a target population [7].
Stratified random sampling was used to select personnel from different area of specialization in order to ensure all categories were adequately represented in the sample. Simple random method was then used to select respondents from various strata. There were a total of 150 (88.23%) specialist in the sample which included 95 from ICT organizations and 55 from MIS department of higher institutions. In the sampled institutions, 25 ICT lecturers were randomly selected, making a total of 170 respondents.

2.3 Research Instruments

Questionnaires were used as main instrument for data collection. This is because questionnaires are widely used to obtain information about current conditions and practices and to make inquiries concerning attitudes and opinions quickly and in the precise form [10].

2.4 Validity and Reliability of Research Instruments

Validity is the degree to which a test measures what is supposed to measure [9] and reliability is the degree to which a test consistently measures whatever it measures [11]. In this study, validity of the questionnaires was ensured through judgment of experts in teaching, learning, software development and research techniques, while reliability was established through test and re-tests method during pilot study.

2.5 Data Analysis

Data analysis involves some manipulations of data collected through use of statistical tools in order to compute a number, a percentage etc. After data has been collected using questionnaire, it is going to be analyzed using simple frequencies, percentages

2.6 Response Rate

To ascertain in-depth of data collected, stating response rate of respondents is essential. Out of one hundred and seventy questionnaires distributed one hundred and twenty (70.6%) were appropriately filled and returned. Fifty (29.4%) were not appropriately filled or returned and therefore were discarded during analysis.
In any research, a return of more than 50% is acceptable [11]. A return of one hundred and twenty (70.6%) for this study was considered acceptable for analysis.

3. RESULTS AND FINDINGS

This section presents results of data analysis and interpretation of research findings. Research results are presented in tables supplemented with some discussions on findings.

3.1 Profile of Respondents

The profile information of respondents included gender, age, experience and area of specialization in PHP applications. Considering the gender of the 120 respondents, 100 (83.33 %) were males and 20 (16.67%) were females which can be shown in Table 1.

Table 1: *Gender*

Gender	No	%
Male	100	83.33
Female	20	16.67
Total	120	100

Also, majority of respondents 65 (54.16%) are 36 - 65 years old followed by 18 - 35 years old which are 45 (37.50%) as shown in table 2.

Table 2: *Age in years*

Age in Years	No	%
Below 18 years	5	4.17
18 – 35 years	45	37.50
36 – 65 years	65	54.16
Above 65 years	5	4.17
Total	**120**	**100**

In addition, Most of the respondents about 80(66.66%) have over 8 years of PHP experience, followed 20 (16.67%) that are between 6 – 8 years of PHP experience and shown in table 3.

Table 3: *PHP Experience*

PHP Experience	No	%
0 – 2 years	5	4.17
3 – 5 years	15	12.50
6 – 8 years	20	16.67
Over 8years	80	66.66
Total	**120**	**100**

Furthermore, majority of the respondents 40(33.33%) are Application Developers, followed by System Designers and Programmers with 30(25.00%) each as shown in table 4.

Table 4: *Area of specialization*

Area of Specialization	No	%
Application Developer	40	33.33
Application Users	5	4.17
System Designer	30	25.00
Programmer	30	25.00
System Analyst	5	4.17
Application Manager	10	8.33
Total	120	100

Lastly, majority of the respondents academic qualifications were Ph.D. holders with 50(41.67%) followed by Master's Degree holders which are about 40(33.33%) of the respondents while 10(8.33%) of the respondent are Bachelor degree holders and 10(8.33%) are HND holders as shown in table 5.

Table 5: *Academic Qualification*

Academic Qualification	No	%
NCE	5	4.17
OND	5	4.17
HND	10	8.33
Bachelor Degree	10	8.33
Master's Degree	40	33.33
Ph.D.	50	41.67
Total	120	100

3.2 Level of PHP Proficiency

In this section first a questions is asked to determine the number of respondents who were conversant with PHP application and how often they make use of the application. The results indicated that in various organization, higher number of the respondents were conversant with PHP applications with about 108(90.00%) while other respondents of about 12(10.00%) rarely use the applications as shown in table 6.

This meant that majority of respondent have the knowledge of the PHP applications. This may be attributed to the fact that PHP application is an open source scripting language, platform independent and widely acceptable and has gain a lot of recognition in Web Application Development Platforms.

Table 6: *Are you conversant with PHP?*

Conversant with PHP	No	%
Yes	108	90.00
No	12	10.00
Total	120	100

The second question is asked to determine how often the respondents make use of PHP Applications. Majority of respondents 105 (87.50%) were recorded using PHP applications always as shown in table 7.

Table 7: *How often do you use PHP?*

How Often do you use PHP?	No	%
Very Often	90	75.00
Often	15	12.50
Sometimes	10	8.33
Rarely	5	4.17
Total	120	100

These findings agreed with assertion that security vulnerabilities are the major challenges of the PHP applications.

3.3 Causes of PHP Security Vulnerabilities

A question was asked here to determine the causes of security vulnerabilities in PHP applications and the number of respondents that identify the causes. The results indicated that there are many causes of security vulnerabilities in PHP application. Two causes of the security vulnerabilities, SQL injection and source code revelation are been highlighted by the majority of the respondents 75 (62.50%) as shown in table 8 and none of the vulnerability is not highlighted by the respondents.

Table 8: Causes of security vulnerabilities in PHP

Causes of PHP Security Vulnerabilities	No	%
SQL Injection	75	62.50
Remote File Inclusion and Remote File Execution	7	5.84
Cross Site Scripting (XXS)	18	15.00
Session and Cookie Hacking	15	12.50
Directory Traversal	5	4.17
Source Code Revelation	75	62.50

This meant that all the causes provided in the questionnaire were the major causes of the security vulnerabilities in PHP applications. This may be attributed to the fact that PHP application is widely used by both trainers and the professional due to the open access and user friendliness of the PHP application.

3.4 Challenges of PHP Security Vulnerabilities

Another question was asked to determine the challenges faced while using of PHP Applications in terms of security vulnerabilities. Majority of respondents 80(66.67%) were recorded to be having database hacking challenges, followed by 25(20.83%) of the respondents which were infected with malicious client-side script, and the remaining 15 (12.50%) respondents were facing other challenges provided as shown in table 9..

Table 9: Challenges faces due to security vulnerabilities in PHP

Challenges Faced	No	%
My database was hacked	80	66.66
I discovered that unknown party is running codes on my web server and client-side	5	4.17
My site was infected with malicious client-side script	25	20.83
Unknown party hacked into my user session and cookie	5	4.17
Unknown party access the restricted files on my server and execute some command	5	4.17
Total	**120**	**100**

3.5 Solutions to PHP Security Vulnerabilities

This is a question to determine the methodology used to resolve the security challenges of the PHP application. Higher number of the respondents 90(75%) adopted a method of ensuring that all data input are validated, verified and cleaned up before it can enter the application and also restricted user privileges to an absolute minimum. About 20(16.66%) of the respondents adopted a method of using security software to secure PHP application and also incorporated security platform in PHP application that validate & sanitize all user input by removing all suspected data & filtering out meta-characters and the remaining and 10(8.33%) adopted other methodology provided in the research questionnaire as shown in table 10.

Table 10: Solutions to security vulnerabilities in PHP

Solutions	No	%
I used security software to secure my application.	15	12.50
I incorporate security platform in my application that validate & sanitize all user input by removing all suspected data & filtering out meta-characters.	5	4.17
I used SSL secured connection to protect the handling of sensitive information and prevent session and cookie	5	4.17
I restricted user privilege to an absolute minimum	20	16.66
I turned OFF the register_globals directives	5	4.17
I ensured that all data input are validated, verified and cleaned up before it can enter the application	70	58.33
Total	**120**	**100**

3.6 Rating of PHP in Terms of Portability and Accessibility

In this section a questions was asked to rate PHP application in terms of portability and accessibility.

The results indicated that portability and accessibility is one of the major key factor driving high PHP applications development because majority of the respondents 110(91.66%) rated PHP applications as one of the most portability software development application while other respondents of about 10(8.33%) rated it otherwise as shown in table 11.

Table 11: Rating of PHP in terms of portability and accessibility

PHP Portability and Accessibility	No	%
Very Good	60	50.00
Good	50	41.67
Fair	5	4.17
Poor	5	4.17
Total	**120**	**100**

3.7 Rating of PHP in Terms of Security

A question was asked here to rate the security level of PHP. The results indicated that PHP applications are still more secured compared to other software development application because most of the respondents 109(90.84%) rated PHP application as much secured application while other respondents of only about 11(9.17%) rated it as unsecured application as shown in table 12.

Table 12: Rating of PHP in terms of security

Security	No	%
Very Secured	80	66.67
Secured	29	24.17
Unsecured	11	9.16
Total	**120**	**100**

3.8 Rating of PHP Compared to Others

Here a question was asked to rate PHP applications to other web development applications. The results indicated that PHP application is widely used and also with the fact that is open source software it has a lot of supports by different developers from various part of the word. It is as well user friendly. This is because majority of the respondents 111(92.50%) reviewed and rated PHP as best application compared to other applications, while the other respondents of about 9 (7.50%) rated it otherwise as shown in table 12.

Table 13: Rating of PHP compared to others

PHP Compared to Others	No	%
Best	50	41.67
Better	40	33.33
Good	21	17.50
Fair	9	7.50
Total	**120**	**100**

3.9 Rating of PHP by Ease of Operation

Here also a question was asked to rate the operation of PHP applications. The results indicated that PHP is user friendly and the friendliness of PHP makes the operation easy and not cumbersome. Majority of the respondents 100(83.33%) rated PHP as a user friendly application while the other respondents of about 20 (16.67%) rated it as difficult application to operate as shown in table 14.

Table 14: Rating of PHP by ease of operation

PHP Ease of Operation	No	%
User Friendly	100	83.33
Difficult	20	16.67
Total	**120**	**100**

3.10 Limitation of PHP

Furthermore a question is asked to review the limitations of PHP in terms of software development and scripting language. The results indicated that many of the respondents 70(58.33%) were recorded not to have limitation with PHP, while the other respondents of about 50(41.67%) were recorded to have limitation in what they can use PHP scripting language to develop as shown in table 15.

Table 15: Limitation of PHP

Limitation of PHP	No	%
None	70	58.33
Some things	28	23.33
Many things	22	18.34
Total	**120**	**100**

3.11 Solutions to Security Vulnerabilities in PHP Applications

The IT professionals who responded to this question give some valuable insights on how to overcome security vulnerabilities in PHP application.

As shown by table 16, 96 (80%) suggested secured connection like SSL is used to handle sensitive Information, 105 (87.50%) suggested all data to be inputted from server and client-side should be validated, verified, cleaned up and remove all suspected data before it can enter into the database, 110 (91.67%) suggested that developer should ensure user-level priority and give less privilege to user accounts and 115 (95.83%) suggested that developer should use all the appropriate security measures and function to secure the application i.e. using ESCAPE FUNCTION, Turned OFF register_globals directive etc as shown in table 16.

Table 4.15: Security recommendations for PHP developers

Security Recommendations	No	%
They should ensure that secure connection like SSL is used to handle sensitive Information	96	80.00
They should ensure that all data to be inputted from server and client-side are validated, verified, cleaned up and remove all suspected data before it can enter into the database	105	87.50
They should ensure user-level priority and give less privilege to user accounts	110	91.67
They should use all the appropriate security measures and function to secure the application i.e. using ESCAPE FUNCTION, Turned OFF register_globals directive etc.	115	95.83

These results found that the best solution to security vulnerabilities in PHP Application is use of all the appropriate security measures and functions to secure the PHP applications like ECAPE FUNCTION, turn off register_global directives, etc.

4. CONCLUSION

This research surveys the security vulnerabilities in PHP Application among IT professionals in Nigeria. We target 170 IT Professionals in various ICT organizations and institutions in Nigeria. The main instrument for data collection was questionnaire. Stratified random method was then used to select respondents from various strata in which there were a total of 170 specialists in the sample which included 95 from ICT organization, 55 from MIS department of higher institutions and 20 ICT lecturers were randomly selected. The data collected from questionnaire were analyzed using simple frequencies and percentages. Out of 170 questionnaires distributed 120 (70.6%) were appropriately filled and returned. 50 (29.4%) were not appropriately filled or returned and therefore were discarded during analysis.

Considering the profile of the respondents, majority of the respondent are male (83.33%), aged 36 – 65 years old (54.16%) followed by 18 – 35 years old (37.5050, having over 8 years PHP experience (66.66%) followed by 6 – 8 years of experience (16.67%), application developers (40.00%) followed by Designers and Programmer with (25.00%) each and are Ph.D. Holders (41.67%) followed by Master's Degree (33.33%).

In addition, higher numbers of respondent are conversant with PHP (90.00%) and using PHP always (87.50%). Furthermore, two causes of the security vulnerabilities, SQL injection and source code revelation are been highlighted by the majority of the respondents 75 (62.50%). Majority of respondents 80(66.67%) were recorded to be having database hacking challenges. And 95.83% of the respondents suggested that developer should use all the appropriate security measures and function to secure the application i.e. using ESCAPE FUNCTION, Turned OFF register_globals directive etc.

PHP has also been rated in terms of security, ease of operation and compared to other applications. So, 91.66% rated PHP applications as one of the most portability software development application, 90.84% rated PHP application as much secured application, 83.33% rated PHP as a user friendly application, 92.50% reviewed and rated PHP as best application compared to other applications and 58.33% were recorded not to have limitation with PHP .

Lastly, this research can be improved to cover IT professionals worldwide. This may be accomplished by creating an online questionnaire for all IT professionals worldwide to give their opinions on the security vulnerabilities in PHP applications.

REFERENCES

[1] Andrews, M.: "The State of Web Security". IEEE Security & Privacy, vol. 4, no. 4, pp. 14-15 (2006).

[2] D. Balzarotti, M. Cova, V. Felmetsger, N. Jovanovic, E. Kirda, C. Kr¨ugel, and G. Vigna. Saner: composing static and dynamic analysis to validate sanitization in web applications. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, May 2008.

[3] N. Jovanovic, C. Kruegel, and E. Kirda. Pixy: A Static Analysis Tool for Detecting Web Application Vulnerabilities (Short Paper). In Proceedings of the 2006 IEEE Symposium on Security and Privacy, pages 258–263, Oakland, CA, USA, 2006. IEEE Computer Society

[4] .V. B. Livshits and M. S. Lam. Finding Security Errors in Java Programs with Static Analysis. In Proceedings of the 14th USENIX Security Symposium, pages 271–286, Aug 2005.

[5] G. Wassermann and Z. Su. Sound and Precise Analysis of Web Applications for Injection Vulnerabilities. In Proceedings of the ACM SIGPLAN 2007 Conference on Programming Language Design and Implementation, San Diego, CA, USA, Jun 2007. ACM.

[6] Bello Alhaji Buhari, Ahmad Idris Tambuwal "Security Enhanced Online Registration Prepaid Scratch Card Payment Approach" Journal Of Engineering and Technology Research, Scientia Library Volume 2, Issue 6, December 2014 page 53-59

[7] Sekaran U. (2007) Research methods for business and skill building approach (4th ed.). Willey India. Simonson, M. (2008) Technology use of Hispanic bilingual Teachers: A function of their beliefs, attitudes and perceptions on peer technology use in the classroom, Journal of Instructional Technology 31(3) 257-266

[8] Orodho, J. A. (2008). *Techniques of writing Research Proposal and Reports in Education and social Sciences.* Maseno: Kanezja.

[9] Gay, G. (2002). Preparing for culturally responsive teaching. **Journal of Teacher Education, 53** (2) 106-116.

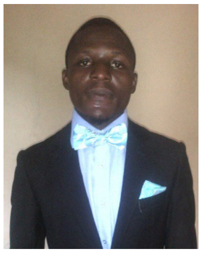
[10] Kombo, D. K., & Tromp, D. L. (2006). Proposal and thesis writing: An introduction. *Nairobi: Paulines Publications Africa*, 10-45.

[11] Mugenda & Mugenda (2003) Research Methods: Acts Press, Nairobi.

Author's Biography

OYEMADE, Olufemi Isaiah, was born on the 18th of March, 1985, in Ife East Local Government of Osun state. He hails from Osun State of Nigeria. He obtained his Primary school leaving certificate at All Saint Nursery and Primary school, Ile-Ife, between 1991-1996. He proceeded to Urban Day Grammar School Ile-Ife, between 1996 and 2002, thereby obtaining his Secondary school leaving certificate. He went ahead to obtain a Bachelor's degree in Computer Science and Information Technology from Usman Danfodiyo University, Sokoto, Sokoto state from 2008-2011. He has just completed his Masters' degree in Information Technology at National Open University of Nigeria. He is currently Regional Passive Planned Manager (IHS Towers) at BISWAL LIMITED, a position he has held since 2012.

Bello Alhaji Buhari was born on 20th October 1974 in Sokoto North Local Government of Sokoto State. He obtained his Primary certificate at Model primary school Wurno road Sokoto from 1981 – 1987. He proceeded to G.S.S.S Yelwa Yauri where he obtained his junior leaving certificate from 1988 – 1990. He also obtained his senior secondary school certificate at Nagarta College Sokoto from 1991 – 1993. He then obtained a B.Sc. Degree in Computer Science at Usmanu Danfodiyo University Sokoto from 1996 – 2000. He further obtain an M.Sc. Degree in Computer Science at Ahmadu Bello University Zaria from 2006 – 2009. He is now undergoing Ph.D in Computer Science Research at Ahmadu Bello University Zaria. He started his career as a lecturer at Sokoto Polytechnic from sept 2003 to Dec 2003. He is presently lecturing at Usmanu Danfodiyo University Sokoto from Jan 2004 to date.



ODIAGBE, Justus Oluwaseun, was born on the 7th of April, 1990, in Ijebu ode Local Government of Ogun state. He hails from Edo state of Nigeria. He obtained his Primary school leaving certificate at St. Anthony's Nursery and Primary school, Ijebu-Ode, between 1993-2001. He proceeded to Sacred Heart Catholic College, also in Ijebu-Ode, between 2001 and 2007, thereby obtaining his Secondary school leaving certificate. He went ahead to obtain a Bachelor's degree in Computer Science and Information Technology from Bowen University, Iwo, Osun state from 2008-2012. He has just completed his Masters' degree in Information Technology at National Open University of Nigeria and he is currently rounding off his Masters' in Educational Leadership and Administration, at University of Nicosia, the course which being taken in an online environment. He is currently an ATM Engineer (NCR and Hyosung brands) at Inlaks Computers Ltd, a position he has held since 2013.