ISSN 2047-3338

Securing Enterprise Information Using Dual Combat Technique

Erike A. I[1], Inyiama H.C[2] and Nwalozie G.C[3]

[1,2,3]Department of Electronic and Computer Engineering, Nnamdi Azikiwe University, Awka Anambra State, Nigeria

[1]zubyerike@gmail.com, [2]hc.inyiama@unizik.edu.ng, [3]gc.nwalozie@unizik.edu.ng

Abstract– **Enterprise Information Portal is a gateway through which every employee in the enterprise gets access to personalized information in the organization. Information security has been a problem in many organizations which has led to many organizational loses. Security of enterprise data in organizational databases therefore becomes a thing of utmost importance since no organization can work well without viable information. This research work is focused on securing Enterprise Information Portals against Username enumeration attack and Brute-forcing Password attack using Dual Combat Technique. Structural System Analysis and Design methodology was used to design the security framework which gives users the privilege of locking and unlocking their account immediately an attack is sensed on their account. The following open source technologies were used to implement the development: PHP, MySQL and APACHE. Performance evaluation test which was conducted over the same internet connection condition shows that the new technique alerts the user of an envisaged attack 36.7% faster than the time it takes for the traditional Reverse Turning Test to show up.**

Index Terms– **Enterprise Information Portal, Security, Brute-Forcing and MySQL**

I. INTRODUCTION

IN the recent times, software security has become a global issue with increase in the number of web applications. With vulnerabilities such as SQL injections, Cross-Site Scripting XSS, Username enumeration, Brute forcing of Ids and so on dominating bulleting bill boards, web applications have become the target of all these attacks. It presents an attractive attack target because of their wide entrance point and its potential access to sensitive data such as credit card information, passwords and hidden company's information. To make worse the whole situation, web application developments, unlike other software developments are mostly done by programmers with less security consciousness. Attention is directed more on the workability of the project and not on its robustness.

While security experts routinely bemoan the current state of the art in web application development, application security requirements present yet another hurdle to overcome. Over the years, so much billions of dollars have been lost to information sabotage and other web application security breaches. Along with the increased importance of Web applications, the negative impacts of security flaws in such applications have grown as well. Vulnerabilities that may lead to the compromise of sensitive information are being reported continuously. The cost of the resulting damages is also increasing on daily basis. The main reasons for this phenomenon are time, financial constraints, limited programming skills, and lack of security awareness on the part of the developers. Irrespective of the nature and size of the organization, security has been one of the key areas of importance. Though many works have been done to ameliorate these challenges, yet as web applications continue to evolve, security challenges continue to increase.

Also, some of the solutions earlier proffered by several frameworks were mainly defensive aiming at isolating the application from the attacking vector. With the emergence of Web 2.0 [1], increased information shearing through social networking, websites are often attacked directly. Because of this, industry is to pay increased attention to security of web application themselves as well as security of the underlying computer networks.

II. REVIEW OF RELATED WORKS

According to [2], Portals are "applications that enable companies to provide access to internally and externally stored information, and offer users within and external to the enterprise a single window to personalized information needed to make informed business decisions. An Enterprise Information Portal is a web browser-based system that provides universal access to vital business information in the same manner that internet content portals like Yahoo are the gateway to the wealth of content on the web".

A portal however can be viewed as an avenue to access disseminated information within a company since information chunks can be stored in various systems using different formats. One of the major differences between a traditional website and a portal resides in the fact that the portal is usually customized according to the users' requirement [3]. Because of this unique features of enterprise information portals, there are lots of reasons portals become targets for attackers and hackers. Because of this, there's a necessity to secure web portals in a very crucial way to make sure that information is not tampered with.

Engin et al. [4] described Noxes, a Microsoft – Windows based personal web firewall that runs as a background service in the desktop of a user. Personal firewalls are meant to prompt the user of any connection and thus prompt the user on whether to accept a connection or not. The sole purpose is to allow the user exert control over the connection that the browser is making. This tool allows users to be able to set preferences that the tool is meant to operate on. Though this approach has been applauded with some wonderful results, it is a user-security framework against cross site scripting attack.

Secondly, it takes a knowledgeable user to be able to detect which URL is malicious or not so as to either allow or disallow it. Every other user can as well parse such malicious code and end up exposing information to the supposed attacker. The web application on its own has no robustness over such attacks.

Following the research carried out by [4], a hybrid analysis framework for detecting web application vulnerabilities was described by [5]. Their work was targeted at monitoring and interception of injection attacks. The hybrid analysis involved both statically analysing web applications to spot dangerous statements and dynamically monitoring identified statements. This step involves the development of a program model for each program function in the form of a control program graph (CGF). This when aggregated together would form an inter-procedural CGF that is analysed to individuate all possible code paths from a user input source to a sensitive sink. When those variables are analysed, only those that can affect the input argument of a sensitive sink are extracted. As the program runs, only dangerous statements need to be monitored against. Dangerous statements trapped are used to perform an efficient taint analysis. The work done was well crafted and extended PHP 5.2.6. This means that the analyser can be integrated into the future versions of PHP and be made available for anybody using the newer version. That notwithstanding, the static engine can be greatly improved by integrating a static taint analysis. More so, this engine significantly, would track down SQL injections in the sites.

In the work done by [6], Securing passwords against Dictionary attacks, the authors proposed an idea such that once the user has successfully logged into an account using the normal username-password authentication method, the server places in the user's computer a cookie that contains an authenticated record of the username, and possibly an expiration date of the cookie. "Authenticated" means that no party except for the server is able to change the cookie data without being detected by the server. This they stated can be ensured, for example, by adding a Machine Access Code (MAC) that is computed using a key known only to the server. Cookies of this type can be stored in several computers, as long as each of them was used by the user. The login form was designed to function in three perspectives:

1. The user enters a username and a password. If his computer contains a cookie stored by the login server then the cookie is retrieved by the server.

2. The server checks whether the username is valid and whether the password is correct for the username that was entered.

3. If the username/password pair is correct, then

(a) If the cookie is correctly authenticated and has not yet expired, and the user identification record stored in the cookie agrees with the entered username, then the user is granted access to the server.

(b) Otherwise (there is no cookie, or the cookie is not authenticated, or the user identification in the cookie does not agree with the entered username) the server generates an RTT and sends it to the user. The user is granted access to the server only if he answers the Reverse Turning Test correctly. This condition means that the server does not recognize the machine that is demanding access to it, probably because it is its first time of accessing it.

4. If the username/password pair is incorrect, then the user is immediately denied access.

According to them, the decision of whether or not to serve an RTT must be a deterministic function of the entered username/password pair. That is, for any specific pair of username and password values, the user is either always asked to pass an RTT, or is never asked to answer one.

This method of securing password against dictionary attacks actually solved a lot of difficulties which has been encountered when it comes to the issue of signing into a web application. First, dictionary attacks were controlled by the introduction reverse turning test, which is a kind of agent-based test that generates random and irregular puzzles that can be easily solved by humans but difficult for intelligent agents. By generating different RTT for each failed login attempt, dictionary attack is minimized. But this same problem posed a problem of annoying legitimate users with the RTT each time they want to login. So in order to curtail this difficulty, they proposed the use of cookies to temporary store authenticated information of username and password on the user's machine each time there's a valid authentication but throws the RTT whenever there's a fresh login or logging from another computer.

This idea is highly appreciated but cannot protect the system against global attack – a situation where the user comes with a lot of valid usernames and begins to try out the username alongside some random passwords. For the fact that the attacker has not made a repeat of the same username/password combination, the system does not throw an RTT for the attacker. Even if it does, there can be a deliberate answering of the RTT and still the system continues to be vulnerable. Also, the researcher did not take into cognizance if the user disables cookies in his computer. More so, some developers do not use cookies in their development due to security vulnerability associated with it. Cross site scripting attack is mostly targeted at stealing the cookie information and later using the same to login as if the attacker were a legitimate user.

This current research work presents a dual technique of combating attacks targeted at web portals either by brute-forcing of user's account or passwords using either the manual method or by dictionary attack without the use of denial of service scheme to lock out users from accessing the application.

In this technique, though the administrator has powers to stop a machine from attacking the system and also locking out users when an attack is envisaged on their user account, the second part of this privilege is relinquished to the user on a real-time bases. In other words, this technique gives the user the legitimate right to lock his account whenever he is notified of a threat and also a way to unlock his account when he decides to. This will solve the problem encountered in the past in some auction sites where rivals deliberately attack their opponent's account, so that the site's security feature will lock the rival out of service and leaving the malicious attacker with no competitor.

III. METHODOLOGY

Structured Systems Analysis and Design Method (SSADM) is used in this work, this is because its usage is expedient for those who work with enterprise organizations as it is considered the standard for these organizations.

SSADM is based on the data flow diagrams as shown in Fig. 1. At the early stages of projecting and description of models (functional, informational and event-trigger) the top-down method is used. At the description of data flows out of the system and into the system, data flow diagrams, which denote system boundary, are used.

At the description of data models Logical Data Structure (LDS) diagrams are used. LDS describes which data the system operates with. It is created for existing system and also is added at the development of the new one.

For modeling events, which happened in the system, Entity Life History (ELN) diagrams are used. These diagrams support states indications and the possibility of description not only consecutive but parallel or reiterative events and also description of the choice of events course. ELN describes how data change in the system in the course of time at different variants of events.

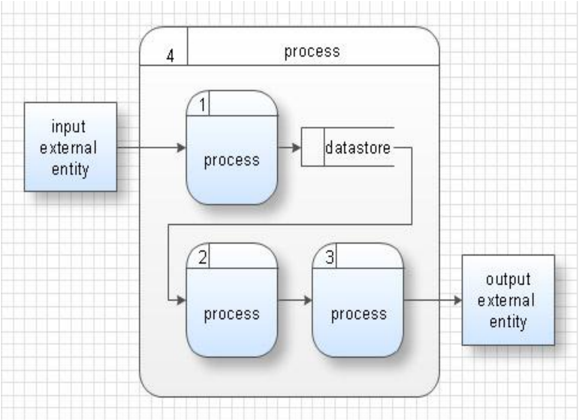


Fig. 1: Process flow diagram

The analysis, projecting and documenting of information system according to SSADM involves 6 main stages. Each stage is further divided into several steps that define tasks which should be fulfilled at that given stage. The system is studied for getting system requirements. Detailed project is created on the logic level and then transformed into the physical project [7].

SSADM stages:

- Analysis of the existing system or estimation of practicability. This involves the analysis of the existing system and creation of DFD for visualization of known problems and system description. If the system is developed from the beginning then the projecting starts from definition of new system requirements.
- Requirements definition. On the basis of available data about the system functions, which the system must execute are clearly defined. Also boundaries of the future system and data which will be processed by the system are defined. Information logical model of requirements is constructed.
- Definition of technical requirements and device equipment cost. Definition of the expected profit with the introduction of new functions.
- Development of logical data model. Specification of the list of functional requirements. After development of the logical project the adding of new requirements on SSADM is forbidden. Only correction of the existing requirements, their specification and concrete definition are allowed.
- Projecting of logical requirements. Specification of requirements.
- Physical projecting. Physical information model and specification to program elements are developed and optimized. Specifications to program elements are specified and documentation is drawn up.

The Choice of this design methodology is based on its precise definition and support of so-called "non-functional requirements" and simplicity of application. It is also best fitted for the work because it will give room for future projection and planning.

The Enterprise Information Portal Architecture

The architecture for the Enterprise information Portal is presented in Fig. 2. The figure presents three tiers for EIP implementation which are the client tier, the application tier and the data tier. These tiers are further expatiated.

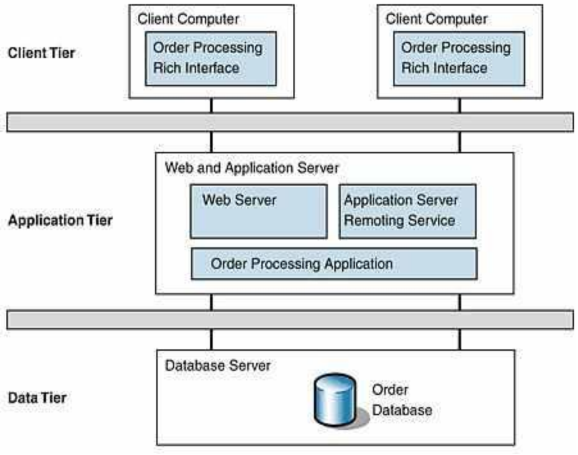

Client Tier
Client Computer
Order Processing Rich Interface
Client Computer
Order Processing Rich Interface
Application Tier
Web and Application Server
Web Server
Application Server Remoting Service
Order Processing Application
Data Tier
Database Server
Order Database

Fig. 2: Three tier architecture for the web portal

Client Tier: The client interface is the point where the portal users use to interact with the company's portal. Here, the user's computer; the GUI (Graphical User Interface) is majorly the point of communication with the portal. Information as it relates to the user is communicated to him through the user interface. This area was implemented using some client side technologies like HTML (Hypertext mark-up language), CSS (Cascading style sheet) JavaScript etc.

Application tier: This holds the intermediate application that runs between the clients' interface and the database. Here resides the web server and probably the application server. The server side applications also run on this tier of the architecture. The web server gets the user information from the user interface through the help of the application, processes it and submits same to the database and also gets information according to the user's request from the database and shows to the user via the user interface. This was achieved using some server side scripting technologies like ASP.NET, PHP, Ruby on Rails etc and server technologies like Apache, Tomcat etc.

Data tier: Data tier deals with databases - enabling collection of data arranged to provide efficient retrieval. Data here are managed by properly storing the data in designated tables, and right relationships built to ensure seamless retrieval. The database technology is enhanced by the use of Database Management System (DBMS) - software for accessing databases. Some of the available DBMS in use include: DB2, MS SQL, MySQL, ORACLE, ACCESS etc. But, Mysql is used for this work.

IV. SYSTEM MODELING AND DESIGN

The combat system design block diagram is as in Fig. 3. It basically comprises of three blocks: the input block defines the supposed attacking vector used as a handle to break the security of the system. The second block holds the module that will analyse the attack to:

1. Know the type of attack that it is.
2. Route it to the desired combat module where proper action will be taken to combat the attack.

This combat module is represented by the third block of Fig. 3.

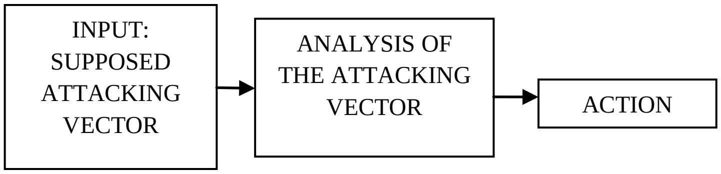

INPUT: SUPPOSED ATTACKING VECTOR
ANALYSIS OF THE ATTACKING VECTOR
ACTION

Fig. 3: Block diagram of the combat system

The dual combat system works basically in structural step in which each action is taken depending on the state of the previous action.

Step One: The crime detector logic system is required to send notice to users when unauthorized access is detected upon signing into the user account. Crime is envisaged when a user does not enter the correct clearance parameters when trying to log into his or her account. Upon first and second trial, the system assumes that the person trying a login attempt may not be the legitimate user, then, the detector logic system is required to issue a clearance test (Reverse Turning Test (RTT)) when the iteration count of wrong entry is up to three (3).

Step Two: When the alarm status becomes high, two parallel combat techniques are activated simultaneously though at different entry counts.

a) The detector clearance system will immediately issue a clearance test (Reverse Turning Test) which is a test given to the user to answer correctly before access is granted for him to try to log in again. From this time on as the user wants to login throughout that session, he would be required to pass the Reverse Turning Test. This is meant to stop dictionary attack (That is an automated login that is being carried out by intelligent agents). Immediately, the user will be alerted on a real time basis that his account has been tampered. When this is done, the user will have the option of locking up his account temporarily. Until the option to temporarily lock up his account is set, he will not be prompted to unlock his account.

b) Another alarm status is issued in addition to the previous one when the listener index records a-5-successive attempts from the same address. This means that a global attack is envisaged. At this time, a malicious person is trying to deliberately break into a user's account by trying out different passwords from the comfort of his personal machine. At this point, Denial of Service Combat is automatically raised by the system to stop the attacker by redirecting him away from the application.

Modelling

There are two parameters involved in this system of which both values must be set to high before access is granted. These are: Username denoted by U and Password denoted by P. The possible states of these parameters by digital logic are illustrated in the Table 1.

According to Table 1, State One denotes a trial when the Username and Password are both wrong. State Two denotes a trial when the Username is wrong and the Password correct. State three is a trial where the Username is correct and Password is wrong. Then the final State is a trial when the Username and Password are both correct. And this is the state of no attack.

Table 1: Parameters possible logic states

	U	P		Denotes
State One	0	0	$U^1.P^1$	Attack Envisaged
State Two	0	1	$U^1.P$	Attack Envisaged
State Three	1	0	$U.P^1$	Attack Envisaged
State Four	1	1	UP	No attack, login OK.

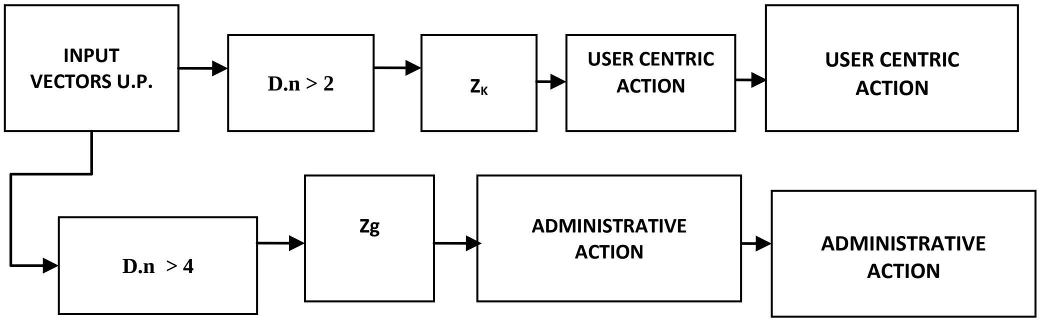


Fig. 4: Model of the dual combat technique

From Table 1, the system is required to give an output alert and trigger an action when the entry vectors take any of states one, two and three for three consecutive times. Hence output:

$$Z = (U^1.P^1 + U^1.P + U.P^1) \qquad (1)$$

Let $U^1.P^1 = x$

$U^1.P = y$

And $U.P^1 = z.$

Then $Z = (x + y + z) \qquad (2)$

Note that the plus (+) sign in the expression does not represent an operator for addition but rather a logical 'OR' symbol.

Let $D = (x + y + z)$

Therefore $Z = D$

The detection expression can thus be written as

$Z = D.n$

Where n = the number of iteration of any of the above conditions before an alarm signal is issued. Thus;

For dictionary attack combat,

Dictionary attack ZD = D.n>2

While for Global attack;

Global attack ZG = D.n>4

x,y,z represent the logical states of the input vector.

$x = U^1.P^1$ represents the state where the input vectors are both wrong or does not exist.

$y = U^1.P$ represents the situation when the input vector U alone is wrong.

$z = U.P^1$ represents a true input vector U and wrong input vector P.

Therefore, the model for the proposed technique is as in Fig. 4.

V. TESTING AND EVALUATION

Two broad approaches were used to test this work. The first was the bottom-up approach which was used to test every program modules, the subsystem and the entire system. The program modules were independently designed, tested and implemented. The complete system testing is concerned with finding out errors due to programming and structure. The concern here is to make sure that all the anticipated functions of the system are met.

The input parameter testing was actually the main area of concern. Testing was done to make sure:

a. That the user entered something in the field provided
b. That the format of the input parameter is correct
c. That both parameters exist in the database
d. That the combination of the parameters are correct

Apart from the input parameters, the system is tested to make sure that it is the email address that has been confirmed that was registered, and finally to make sure that database normalization is achieved and that data were successfully entered into the database.

Outputs were designed to be seen both on the graphical user interface (GUI) which included the PC and the user's mobile phone. Acknowledgement was meant to be received for each of the actions performed, in other to be sure that every of the module is working. Links are also tested to make sure that none of the links appearing in the GUI is broken because this may lead to a serious malfunctioning of the system.

A) Performance Evaluation

The system security performance evaluation was conducted to compare the performance of the new technique with that of the traditional RTT (Reverse Turning Test), which is currently implemented by using the 'reCaptcha' API (Application Programming Interface) that is provided by Google. The test was carried out under the same internet connection speed provided by Mobile Telecommunication Network Nigeria (MTN Nigeria) through the use of USB Modem. After the wrong entry has been entered for more than

2 times, many other attempts were made by deliberately entering the right U parameter against wrong P parameters. The results of the response time for only ten attempts are recorded in table 2. Trial attempt is designated by the letter t, while the Dual Technique and RTT response times are represented by D and R respectively. The values of the D and R responses are both in seconds.

Table 2: Comparative responses of Dual Combat Technique and traditional RTT

T (Sequence of trials)	D (Seconds)	R (Seconds)
1	13.24	20.12
2	11.68	13.78
3	9.99	15.99
4	10.48	12.45
5	11.39	13.50
6	31.54	54.16
7	13.48	25.26
8	11.50	31.29
9	10.70	16.50
10	12.39	14.26

From Table 2, the sum of the time responses of the dual combat technique over ten trials is given by$\sum \boldsymbol{D}$.

And the sum of the time responses of the traditional RTT technique over ten trials is given by$\sum \boldsymbol{R}$.

Average time response of the Dual Technique Td is given by:

$$T_d = \frac{\sum \boldsymbol{D}}{\boldsymbol{n}(\boldsymbol{t})} \qquad (3)$$

Where $\boldsymbol{n}(\boldsymbol{t})$ is the number of trials; T_d is the average response time of the dual technique and $\sum \boldsymbol{D}$ is the sum of the D response times.

Average time response of the RTT Technique Tr is given by:

$$T_r = \frac{\sum \boldsymbol{R}}{\boldsymbol{n}(\boldsymbol{t})} \qquad (4)$$

Where $\boldsymbol{n}(\boldsymbol{t})$ is the number of trials; T_r is the average response time of the RTT technique and $\sum \boldsymbol{R}$ is the sum of the RTT response times.

T_r = 21.73seconds

T_d = 13.10seconds

Now, the improvement, 'x' is given by:

$$X = (\boldsymbol{Tr} - \boldsymbol{Td}) \qquad (5)$$

X = 8.63seconds.

Percentage improvement *I* is given by:

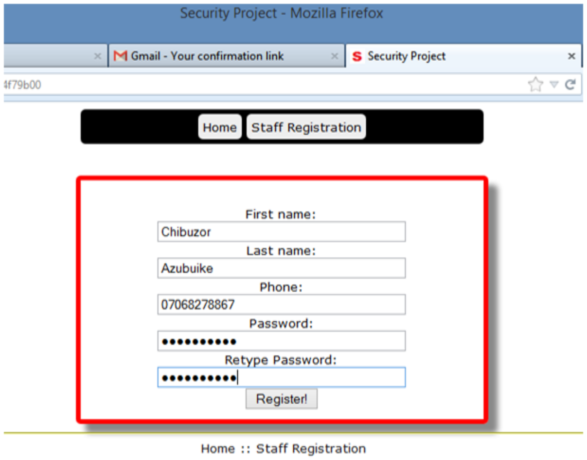
$$I = \frac{\boldsymbol{x}}{\boldsymbol{Tr}} \text{ x } \frac{\boldsymbol{100}}{\boldsymbol{1}} \qquad (6)$$

I = 39.7%

From the tests carried out, it was found that the new technique proved to be 39.7% faster than the traditional RTT in reporting envisaged attack. And, so if the user unto whom the attack is reported to responds immediately, he would definitely be able to block his account against fraudulent accesses.

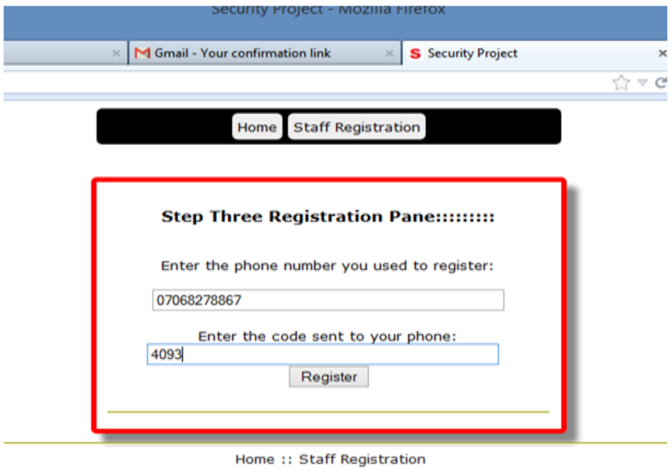
B) Deployment and Maintenance

Once the program was hosted, everybody in the enterprise starts benefitting from the security facility built into the portal to make sure that his account is not hacked into. Maintenance of the system will not be a tedious task since the program is developed using design-by-class technique where one file serves all. Integration of new technologies is easier since the development pattern was designed to be so. There are no file conversions done. Fig. 5 to Fig. 7 show screen shots of the deployed dual combat technique system.


Security Project - Mozilla Firefox
Gmail - Your confirmation link
Security Project
4f79b00
Home
Staff Registration
Register!
Home :: Staff Registration

First name:
Chibuzor
Last name:
Azubuike
Phone:
07068278867
Password:
••••••••••
Retype Password:
••••••••••

Fig. 5: Screen shot of the main registration page loaded from the user's mail box

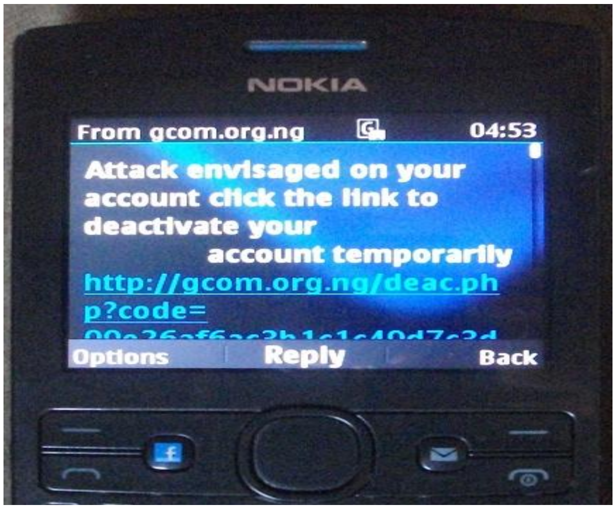

Security Project - Mozilla Firefox
Gmail - Your confirmation link
Security Project
Home
Staff Registration
Register
Home :: Staff Registration

Step Three Registration Pane:::::::::

Enter the phone number you used to register:
07068278867

Enter the code sent to your phone:
4093

Fig. 6: Phone number confirmation page



From gcom.org.ng 04:53

Attack envisaged on your account click the link to deactivate your account temporarily http://gcom.org.ng/deac.php?code=00e26af6ac3b1c1c40d7c3d

Fig. 7: The Phone interface for remote account deactivation

VI. CONCLUSION

A dual combat technique for securing Enterprise Information Portal was developed using Structured System Analysis and Design Methodology. It was implemented using open source technologies ready to be deployed for integration in Enterprise Information Portals and Web Applications in general. This has proved to be efficient in granting users security control over their accounts.

In the course of this work, the system that was developed can be integrated as a security API into every web portal to give the user the privilege of participating in the attack combat process. No user will take up a legal action against any hosting application vendor for locking them out of the application on the grounds of security breaches. Users are now given the privilege of locking up their account and unlocking their account at will just as somebody living in an estate has powers to lock up his apartment before going out.

REFERENCES

[1]. Benny Pinkas and Tomas Sander. “Securing Passwords Against Dictionary Attacks”, STAR Lab. Intertrust Technologies 2014**.**

[2]. Benjamin Livshits and Ulfar Erlingson, “Using Web Application Construction Framework to Protect Against Code Injection Attacks”. Microsoft Research (2007).

[3]. H. Benbya, “Corporate portal: a tool for knowledge management synchronization. “International Journal of Information Management 24” pp 201–220. (2004)

[4]. Engin Kirda, Christopher Kruegel, Giovani Vigna and Nenad Jovanonic. “Noxes: A Client-Side Solution for Mitigating Cross-Site Scripting Attacks” (2006)

[5]. Mattia Monga, Roberto Paleari, Emanuele Passerini, “A Hybrid Analysis Framework for Detecting Web Application Vulnerabilities.” www.security.dico.unimi.it (2014).

[6]. Cenzic “Application Vulnerability Trends Report”.www.cenzic.com/.../cenzic_vulnerability _report_2014 (2014).

[7]. C.S. Odessa ‘Structured Systems Analysis and Design Method (SSADM) with Concept Draw PRO’. http://www.conceptdraw.com/How-To Guide/ssadm 2014

[8]. Symantec, ‘Internet Security Trend Report’, 2013 Trends, Vol.19. www.Symantec.com/Security_response/publications (2013).

[9]. Mudassar Raza, Muhannad Iqbal, Muhammad Sharif and Waqas Haider. “A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication.” World Applied Sciences Journal 19(4), pp. 439-444. (2012)

[10]. Hight C. Inyiama and Rita U. Uzoma Alo, “Software Design and Development: A Practical Approach”. Willy Rose and Appleseed Publishing Company, 2009.