" ANALYSIS OF ATTACKS ON WEB APPLICATIONS SQL INJECTION AND CROSS SITE SCRIPTING AND PRECAUTIONARY AND DEFENCE "
2015-2016

Edgar Subía Ponce
Universidad Técnica del Norte, Carrera de Ingeniería en Sistemas Computacionales, Universidad Técnica del Norte, Avenida 17 de Julio 5-21, Ibarra,
Imbabura, Ecuador.
epsubia@utn.edu.ec

Resumen. Desde el descubrimiento del SEQUEL en el año de 1974, se dio origen al lenguaje que especifica las características de las base de datos que manejaban el modelo relación, es que con este descubrimiento nace el SQL Inyección un ataque que permite encontrar fallas de seguridad y poder modificar casi porte completa de la base de datos, así mismo Cross Site Scripting surge para poder inyectar código malicioso del lado del cliente como del servidor causando gran daño a empresas. El presente trabajo tiene como fin dar a conocer el funcionamiento de los ataques y como poder prevenir las aplicaciones web ante vulnerabilidades encontradas.

Palabras Claves

Seguridad Informática, SQLi Injection, Cross Site Scripting, Ciberdelincuencia, Ethical Hacking, Hacking

Abstract.

Since the discovery of SEQUEL in the year 1974, it gave rise to language that specifies the characteristics of the database that handled the relationship model, is that with this discovery comes the SQL injection attack to find security flaws and power modify almost full bearing of the database, also arises Cross Site Scripting to inject malicious code on the client side and the causing great damage to businesses server.
This paper aims to publicize the operation of the attacks and how to prevent web applications against vulnerabilities found.

Keywords

Security, SQLi Injection, Cross Site Scripting, Cybercrime, Ethical Hacking, Hacking

1. Introduction

In the early 90s the Web had a very easy and simple format that was nothing more than documents planes text that linked together by hyperlinks, today as technology advances, simple documents have been becoming big applications can interact with the user allowing manage and store large amounts of information of any kind, this development has brought in if security problems in the content being published, especially in applications offering services requiring sensitive customer information as they were credit cards, personal data, etc.

For this reason it is used to computer security that is responsible for protecting the data optimally with standards, protocols and rules facilitating minimize possible risks in information. Similarly with the passage of time the Ethical Hacking that helps testing testing computer systems allowing to discover the shortcomings and failures that the developer commits in program coding and server configuration that allows the attacker to compromise security in a born web application also helps to better understand the techniques or more used by hackers, trying to resolve the vulnerabilities that exist in applications in a web environment, methods throughout this study will be understood and may differentiate a hacker true role of a Hacktivist[1].

1.1 Materials and Methods

The use of testing methodologies (pentesting) are very essential because they help assess weaknesses in computer systems, in this case web applications, it consists of a model that reproduces attempts to access a potential intruder from different points entry exist, both internal and remote, to any computing environment. Can detect vulnerabilities in computer systems and correct them quickly and efficiently. At PenTest they are also called Ethical Hacking or Intrusion Test.

1.2 Methodologies to use

For the preparation of analysis has chosen to work with two methodologies the one serving for the development of the demo, and the other is for penetration testing systems.
Development methodology used to prepare the demo is an agile methodology called XP, said method work in pairs and with a maximum group of 10 people where 4 phases are applied:

[1] Hacktivist.- It's all hacker activity motivated by political or social purposes

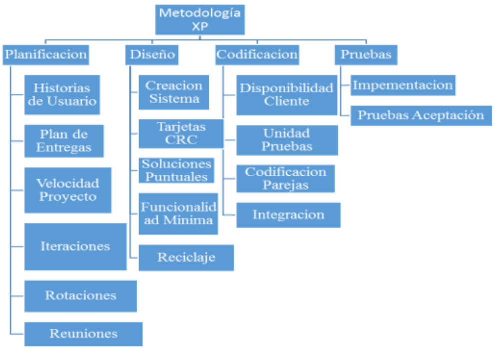


Ilustración 1Metodología XP

Phase 1: Project Planning.
Stories USER.- all customer requirements is collected in NLP language but without details, is used to estimate the effort and the time it took to develop the application. (Gonzalez, 2012) [1]. They are used in the testing phase to observe and verify compliance of development.

Roles.- roles in this work has defined as (Beck, 1999) [2] which were already covered in previous issues.
Delivery.- plan defined the stories that will be used for each version of the program are discussed at this stage take a role the client and the programmer as both decide the time for implementation of the system

Iteraciones.- should define iterations of 3-week application about the beginning of each iteration customers select the user stories according to plan delivery, these stories are divided into tasks that usually lasts 1 to 3 days.

Project.- speed to speed contralateral all tasks are executed at the time indicated by each iteration is used.

The methodology studied Rotaciones.- advised to work together and that helps better the quality and productivity of the developed system.

It is advisable Diarias.- meetings daily to exchange questions and ideas so that the application does not suffer changes and complete the work meetings.

Phase 2: Design.-
Design simple.- Develop a simple, simple design, it helps to understand and reduce time, trying to avoid a lot of effort in development.
Risks.- To prevent risks exist, the methodology proposes to work with a partner.

Re factorizar.- check again and again the code to optimize performance.

Phase 3: Codificación.- At this stage the client plays an important role because most of the time must pass and be aware of the project, the customer is who adds the maximum time in which advances occur.

Phase 4: Pruebas.- two types of tests are performed , the first corresponding to the performance of each version validating and verifying compliance with user stories , and the second call acceptance test where the client or user verifies that its operation . In pentesing methodology called OTP (OWASP Top Project) , which are some steps are performed:

Information Collection.- It is a stage that demands a lot of dedication and time as greater the quantity and quality of information collected , there is the possibility of finding vulnerabilities or backdoors, this stage is integrated within any methodology of testing black box where it is assumed that the attacker does not have detailed technical information used to build the system. To achieve get all the information and platform used there are a variety of resources such as : automated inspection or manual robots, use search engines (Google , Firefox) , recognition parameters GET / POST, detailed discovery platform application and programming languages used .

Management configuración.-Allows an analysis of the architecture and topology of the application, the main objective at this stage is the server that is hosted application , some tests performed at this stage are : verification of certificates both SSL / TLS , Verification on the service data Base (listener connections) in order to search for any type of misconfiguration or "exposure" of sensitive data , Verification extensions pages (* .php, * .asp , * .jsp , etc.) as well as verification of the MIME types supported by the web server

Tests Autenticación.-This type of testing is done in the event that the application contains forms of privileged access for each user can perform tests such as: Verification of credentials traveling on encrypted channels and not encrypted If the application allows the option to "Remember Password " analyze the behavior of such functionality as well as analyze the behavior of other related features, test logoff and Navigation Cache Management .

Management Sesión.- At this stage it involves a very important field is the HTTP protocol as it serves to interact the user to the server and all information is stored you provide , is where the tester performs tests to break and get the sessions user tests related to this stage are: tests on the attributes of the generated cookies to maintain session state on the client side , testing XSS.

Tests Authorization.- Is where the roles, permissions and privileges that a user has to access different application resources are consulted , the tests may be performed: Try to avoid licensing scheme , Testing privilege elevation to determine if it is possible a user can raise its role and access resources for which initially should not access.

Logic tests Negocio.- long and creativity is used because that is where the tester or intruder verifies the functionality of the system carried out questions like what if , is one of the toughest tests since no support and automated tools to help verify the function of the application , the tester itself must use their knowledge and skills to perform this type of test.

Validation tests data.- A common weakness in applications are validations of the inputs provided by the customer or sometimes the application interface , which is why action must be taken of control over the type of data that is entered into an application , testing performing most common are : SQL injections and injections of JavaScript code.

Testing Denial of Services.- Basically it is saturated with requests to the application that is server side . The tests most commonly used for this type of testing is blocking user accounts, storing too much data in session

Testing Services Web.- The vulnerabilities that exist in this type of tests are oriented more to the XML files that are exchanged with the client and the server, the tests used in this type of testing is testing the structure of XML.

tests Ajax.- Is a technique that is widely used in web pages to boost responses server side, a technique used for this type of evidence is proof Ajax vulnerabilities , specifically those related to the XMLHttpRequest object.
Note that in this section of the methodology validation testing SQL Injection and XSS to data is used.

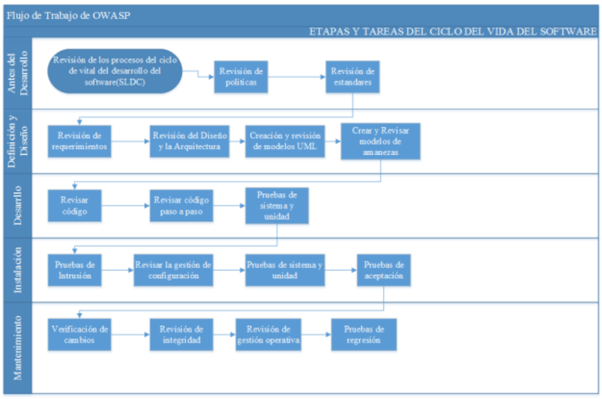

Flujo de Trabajo de OWASP
ETAPAS Y TAREAS DEL CICLO DEL VIDA DEL SOFTWARE
Antes del Desarrollo
Revisión de los procesos del ciclo de vital del desarrollo del software(SLDC)
Revisión de politicas
Revisión de estandares
Definición y Diseño
Revisión de requerimientos
Revisión del Diseño y la Arquitectura
Creación y revisión de modelos UML
Crear y Revisar modelos de amanezas
Desarrllo
Revisar código
Revisar código paso a paso
Pruebas de sistema y unidad
Instalación
Pruebas de Intrusión
Revisar la gestión de configuración
Pruebas de sistema y unidad
Pruebas de aceptación
Mantenimiento
Verificación de cambios
Revisión de integridad
Revisión de gestión operativa
Pruebas de regresión

Ilustración 2 Test de Seguridad en el ciclo de desarrollo de una aplicación

2 Development Tools

2.1 Kali Linux

It is a free Linux distribution based on Debian and developed by an organization called Offensive Security experts audit and security , is a project that was created by another project called backtrack that is currently out of service because joined with kali . Kali , now has more than 300 programs for the implementation and verification of attacks , basically corresponding with computer security and not for computer crime , with some of the best known Nmap (a port scanner) , Wireshark (a sniffer), John the Ripper (a password cracker) and Aircrack-ng (Software security testing wireless networks) suite, in addition to the Metasploit framework , used to find vulnerabilities in web especially focused on computer systems.

2.2 Leguaje PHP

It is a high-level language and runs server-side and was created to implement static , interactive and dynamic web sites can create a variety of web pages deicide which has a lot of bookstores , including its functionality allows you to connect with relational database.(Anabell, 2004)[3]

2.3 Servidor Apache

It is a program that runs the server side, it is open source and can be run on various platforms such as Linux , Microsoft and Mac . Note that this server is the most widely used globally due to its high stability , versatility and reliability. (Asensio Hildago , 2014) [4]

2.4 Framework Symfony

It is a framework that uses a PHP MVC design pattern , Symfony is a complete framework designed to optimize, thanks to its characteristics , the development of web applications. To begin with, separates the business logic , the logic of the presentation server and the web application. (Fabien Potencier , 2013) . [5]

This framework uses some very useful components to improve and optimize the development and are as follows :

Tabla 1 Componentes de PHP y Symfony

COMPONENTES	**DESCRIPCION**
ORM	is a relational mapper object used in programming to transform into classes, attributes and data , all columns tables and relationships in a database.
DOCTRINE	It is a library mimicked hibernate, which helps

	create a persistence layer to work with objects in php.
DQL	It is a query language based on doctrine , it is similar to SQL statements and is used for objects instead of tables.
YAML	File format serialization it is working with native data programming languages

Fuente: Autoría Propia

2.5 Database Postgresql

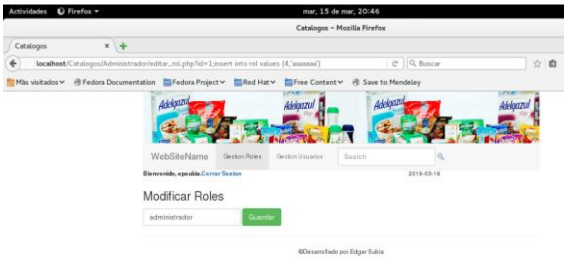
It is a database engine DBMS data used to create and access data , consists of a DDL language, a DML and SQL , and needs the help of an interpreter as it is pgadmin used to interact and with the database . POSTGRES pioneered many concepts that was only available in some commercial database systems much later data. (Momjian , 2014) [6]

3 Vulnerabilities

A vulnerability is a weakness in a system either software, hardware , data, the latter are the most important within an organization because they do not they can be and to repair other components if they can be repaired when there is weakness an attacker can break integrity and commit fraud , altering applications, vulnerability occurs because a bug in the application or a failure in coding or sometimes careless user to remember your passwords in browsers.

3.1 Sql Injection

It is a method widely used worldwide to detect abnormalities in web applications, this method is in communication with the database using SQL statements through a web browser , which aims to extract possible information that is stored in a database data. (De La Quintanaillanes , 2013) . [7]



localhost/Catalogos/Administrador/editar_rol.php?id=1;insert into rol values (4,'aaaaaaa')

Modificar Roles

administrador

Ilustración 3 Inyección con dato numérico

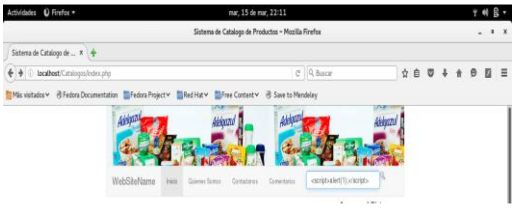
3.2 Cross Site Scripting

This attack as above studied is very powerful and dangerous as it is operated on the client side and not the server, so that user security is very vulnerable and exposed to various frauds. This method involves injecting HTML or JavaScript code into a web application whose goal is is that the user's browser to run the injected when viewing the altered page code. XSS commonly used to cause undue action on a user's browser, but it depends XSS attack that is done, you can exploit the failure of a server or the application itself. The XSS can be used to phishing, theft of credentials, troyanizar browsers, or simply to make a deface, everything depends on the page.

There are two types of XSS

• Persistente.- Such attacks occur when there are security holes, the server generates a snapshot page of results according to information provided, an example can be in the search fields.

• Reflejado.- The information provided by the user is stored in the database, file system or any other place that cause much harm, then that information is displayed to other users to visit the page so it is known to this attack as persistent. With this type of attack what can be done it is to steal cookies, an example where you can find these vulnerabilities are discussion forums.



localhost/Catalogos/index.php

<script>alert(1);</script>

Ilustración 4 Inyección XSS en validaciones de texto

4 Conclusions

• Apply a good methodology to help verify pentest risks and vulnerabilities , and correct the most common mistakes when programming comment .

• The vulnerabilities studied cause much damage and affect the entire application layer causing loss of vital business information.

• Use testing tools are already free or pay much help serve to determine vulnerabilities.

• Having a well-argued list or log of the current situation of the company serves to realize what state you are and what state of vulnerability is found

.Agradecimientos

Thanks to the Technical University of North for allowing me to be part of this university house and to train as a person with great values and to be a great professional.
A very special thanks to Ing . Mauricio Rea , Director of Labor Grade for giving me his guidance in the preparation of this work degree .

References

[1] GONZALEZ, C. **Análisis,Diseño,Desarrollo e Implementación de una Aplicación Web para la Automatización de Clientes,Vehículos,Facturación,Inventario y Campañas para Autoservicios RBS**. 2012. Departamento de Ciencias de la Computación, Escuela Politécnica del Ejercito, Sangolquí.

[2] BECK, K. Embracing Change with Extreme Programming. **Computer,** v. 32, n. 10, p. 70-77, 1999. ISSN 0018-9162.

[3] ANABELL, C. Java o PHP. **Revista Digital Universitaria,** v. Volumen, 2004. ISSN 1067-6079. Disponível em: < http://www.revista.unam.mx/vol.7/num12/art104/dic_art104.pdf >.

[4] ASENSIO HILDAGO, L. Seguridad en aplicaciones web: una visión práctica. 2014.

[5] FABIEN POTENCIER, F. Z. Symfony 1.4, la guía definitiva. 2013. Disponível em: < http://librosweb.es/libro/symfony_1_4/ >.

[6] MOMJIAN, B. Postgresql. California, p. Documentation, 2014. Disponível em: < http://www.postgresql.org/docs/9.3/static/release-9-3-5.html >.

[7] DE LA QUINTANAILLANES, M. M. SQL INYECTION. **Revista de Información, Tecnología y Sociedad**, p. 38-40, 2013. ISSN 1997-4044. Disponível em: < http://www.revistasbolivianas.org.bo/scielo.php?script=sci_arttext&pid=S1997-40442013000100017&nrm=iso >