UNIVERSIDAD NACIONAL DE SAN AGUSTIN

ANGEL ANDRES BEJAR MERMA

DECEMBER 13, 2020

Web Applications Vulnerabilities

Most Web applications are employed to carry out most major tasks, which includes forms for collect personal, secret and private info such as health history, debit, credit and bank account info as well as user satisfaction criticism.Applications such as educational website, governments' website, healthcare application and financial applications interact with its backend (database) several times upon a client request and there is a compromised in the security of such website and web application.

In this year, In Peru, more than 433 million attempted cyber-attacks have been registered in the first quarter of 2020, where during the months of April and May, the number rose to 7,300 attempted attacks per day, representing an increase of 15%. This according to the Kaspersky (international company dedicated to computer security).

With the increase in the use of financial transactions through cell phones due to social isolation policies to combat the COVID-19 pandemic, attacks known as phishing also increased in Peru.

The Phishing is a kind of Cross Site Scripting that is fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details, by disguising oneself as a trustworthy entity in an electronic communication. Typically carried out by email spoofing, instant messaging, and text messaging, phishing often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site.

In this context three actors can easily be represented the fish, the bait and the hook. These refers to using a bait and waiting for the victims to "take the bait." The baits that are used are varied, for example, a form recommended by a friend or a web page that is trusted but in reality is another.

How does it work?

The attacker inserts code in one of the fields it can be a typical box with the magnifying glass icon to search for keywords, a space box for participation in a forum, or a data collection form. then the code will run with the XSS vulnerability in the victim user's browser.

Cross Site Scripting has two modes **Indirect**,and **Direct**.

The first attacker enters code in a field of the application can be in a text box of the same website where the victim is, the set of instructions will be executed in the victim's browser, the attacker will obtain valuable information and the victim will not notice.

The second The code that is inserted is not stored on the

web, but is embedded within a link that is somehow sent to the victim to click on it, It is called that because, if the victim finally clicks on the link , the browser will take you to the page in question, which is normally a legal site where the user has an open account, and then it will execute the embedded code, which will try to steal the session cookie, or the data that you enter in the form, or you can even trigger more sophisticated actions on your PC.

With all the ability of the attacker can change in the price of a product transmitted within a hidden field in HTML format, making a fraudulent purchase of a product at a lower price;

Web applications has three-tiered architecture and the communication among the tiers: web browsers provide a user interface, application servers manage the business logic, and back-end databases store the data.Each one of those has.

The basic logic of a website and an internet application which has the client interface and the server end on a webserver and made known by a uniform resource locator (URL). The internet server is understood by its name.

The browser (client) and server talk via a transport protocol TCP. shows the fundamental architecture of data flow in website and a web application.

The transport protocol is HTTP; the data format is Cascading style Sheets (CSS) and hypertext mark-up language (HTML).

The user click or enters a URL to call the application or access the website . A request via communication protocol is sent to the server from the clients.

A script at the net server removes input from the consumer knowledge and creates a request to a backend application server, e.g. a mysql query to a database.

The result is received from the backend by the webserver and returns a hypertext mark-up language (HTML) result page to the consumer. The result is displayed as a page by the client's browser. To show a page, the browser creates an interior picture for it.

Users should take adequate measures to protect themselves

- Do not use public computer, such café computer to login to critical or sensitive websites and web applications.
- Never cache your password and username on a computer
- Always do logoff at end of a session
- Do not use the same password for different websites and web application login details.
- Do regularly change your password for sensitive web application and websites.
- Immediate report and abnormalities in a website or web application service to the provider.

- Ensures that you have personal firewalls and anti- virus installed on your computer and they are up to date

The security of a computer system is important to offer protection to the systems and the data store in it.Now ,in the context of the pandemic It obliges us to use technological tools to be able to communicate in order to carry out banking transactions, purchase records and where users are most at risk of suffering these attacks and compromising both their privacy and their money.An essential fact in web applications and Internet security is that 100 % assurance that a computer system is reliable and confident is not possible. The users They must have the knowledge not to compromise personal information and not give hackers the opportunity to take advantage of the fact that they can reveal secret information or even damage the device with malware.

Another subtle way where privacy comes into play is through cookies, although cookies allow user sessions to be saved on websites, they also save extra information when browsing a website and then show targeted advertising. The user continues and will continue to be a key factor in Phishing, that is why it is important to know how attacks work to verify the reliability of the web application so as not to fall into social engineering.