Abstract: - This paper discusses in detail the main security risks of Web2.0 and their implications over the digital economies. It presents the main vulnerabilities link cross site scripting, cross site request forgery, injection flaws, phishing, information leakage and many more.

Key-Words: - Web 2.0, digital economy, security risks

1 Introduction
Web 2.0 is the novel term, representing the new generation Web applications, such as: start.com, Google maps, Yahoo mail beta and MySpace.com. "Web 2.0" refers to the second generation of web development and web design. This paper analyzes the types of vulnerabilities that Web 2.0 can bring to a business environment. Some people say that Web 2.0 is more “an attitude” than a technology.

The term "Web 2.0" was proposed by Darcy DiNucci in 1999 in [1]. After that, the term was used again in 2003 ([2],[3],[4]).

Web 2.0 has the following characteristics:
- It includes a very large number of applications and services which use the Web as a organized platform for communications
- It is based on an architecture and encourages the active participation of the users;
- It enables the interactions between users with the same interests;
- Offers the following possibilities for the users:
  - To produce content, and share it with other users
  - An experience close to the desktop applications, using friendly GUI’s
  - Public access to databases using API’s
  - Has the ability to connect applications or web services and to aggregate dates from a variety of sources: RSS, blogs;
  - Web 2.0 is about making the “socialization of information” – a concept about applications and

2 Web 2.0 security risks
There are a number of vulnerabilities which came along with this new technology. The main vulnerabilities are:

2.1 Cross Site Scripting (XSS)
In this case malicious input sent by an attacker is stored in the system then displayed to other users. XSS is typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users. Examples of such code include client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy. Vulnerabilities of this kind have been exploited to craft powerful phishing attacks and browser exploits. At risk are blogs, social networks, and wikis.

2.2 Cross Site Request Forgery (CSRF)
Unlike cross-site scripting (XSS) which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser. In CSRFs, the victim visits what appear to be innocent-looking web sites, but which contain malicious code which generates requests to a different site instead. This is happening...
mainly because of AJAX scripts embedded in web pages. Web 2.0 systems' lack of visual feedback make this attack less apparent.

CRSF was used to exploit a vulnerability in Twitter in which site owners could get the Twitter profiles of their visitors. The following things have to happen for cross-site request forgery to succeed:

- The attacker must target either a site that doesn't check the Referer header (which is common) or a victim with a browser or plugin bug that allows Referer spoofing (which is rare).
- The attacker must find a form submission at the target site that does something useful to him (e.g., transfers money, or changes the victim's e-mail address or password).
- The attacker must determine the right values for all the form inputs: if any of them are required to be secret authentication values or IDs that the attacker can't guess, the attack will fail.
- The attacker must lure the victim to a Web page with malicious code while the victim is logged in to the target site.

### 2.3 Injection Flaws
Web 2.0 is vulnerable to all kinds of malicious code injections such as: XML injection, XPath Injection, JavaScript injection and JSON (JavaScript Object Notation) injection. Web 2.0 is often perform some client-side input validation which an attacker can bypass, because rely on client-side code.

### 2.4 Phishing
Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

A phishing technique was described in detail in 1987, and the first recorded use of the term "phishing" was made in 1996. The term is a variant of fishing[5], probably influenced by phreaking[6], [7] and alludes to baits used to "catch" financial information and passwords.

In a phishing attack, a victim receives by e-mail a request to complete an online form with sensitive information, which is then sent to the attacker. The online form is placed on a fraudulent web site. The phishing attack is based on the difficulty of the user to distinguish between the genuine and the malicious web sites.

### 2.5 Information Leakage
Information leakage refers to the leaking of some information to unauthorized parties. This could be happening because of sharing the wrong files over a network, transmitting chat or email messages, etc.

Web Services’ main goal is to provide easy and automated access to information. If not designed and implemented properly, these services may provide access to more information than originally intended, leading to information leakage.

Only very advanced systems employ defenses against information leakage. There are three main ways to do it:

- Use steganography to hide the fact that you're transmitting a message at all.
- Use chaffing to make it unclear to whom you are transmitting messages (but this does not hide from others the fact that you are transmitting messages).
- For busy retransmitting proxies, such as a Mixmaster node: randomly delay and shuffle the order of outbound packets - this will assist in disguising a given message's path, especially if there are multiple, popular forwarding nodes, such as are employed with mixmaster mail forwarding.

### 2.6 Information Integrity
Information Integrity is the trustworthiness and dependability of information. More specifically, it is the accuracy, consistency and reliability of the information content, processes and systems. Information Integrity is a prerequisite for many other information management initiatives. If the underlying information isn’t of a sufficient level of integrity, the success of business activities relying on the information will be limited.

- Insufficient authentication control.
- In Web 2.0 applications the programmers have to check and never trust the content introduced in the system by the users. A novice user can make by mistake some modifications that can be later exploited by hackers. Information systems typically assume there are a small number of privileged accounts that belong to senior or experienced users. A secure system usually ensures that if changes are made by novice users, they need to be authorized before it affects the system.

This vulnerability can be exploited via weak passwords, insufficient anti-brute force controls, clear text passwords, single-sign-on mechanisms.

### 2.7 Insufficient Anti-automation
Insufficient Anti-automation is when a web site permits an attacker to automate a process that should only be performed manually. Certain web site functionalities should be protected against automated attacks.
Left unchecked, automated robots (programs) or attackers could repeatedly exercise website functionality attempting to exploit or defraud the system. An automated robot could potentially execute thousands of requests a minute, causing potential loss of performance or service. For example, an automated robot should not be able to sign up ten thousand new accounts in a few minutes. Similarly, automated robots should not be able to annoy other users with repeated message board postings. These operations should be limited only to human usage. Anti-automation mechanisms like Captchas can help slow down or thwart these types of attacks.

3 Web 2.0 and digital economics

Conducting business in the digital economy means using Web-based systems on the Internet and other electronic networks to do some form of electronic commerce. The electronic commerce or e-commerce is exemplified using Web-based systems buying, selling, and customer service. In e-commerce, business transactions are done electronically over the Internet and other computing networks. The digital economy refers to an economy that is based on digital technologies, including digital communication networks computers, software, and also refers to the convergence of computing and communication technologies on the Internet and other networks, and the resulting flow of information and technology that is stimulating e-commerce and vast organizational change. Web 2.0 opens tremendous opportunities as business models catch up to the technological possibilities.

4 Conclusion

When introducing Web 2.0 into the workplace, it's important to have a good understanding of the types of risks involved. AJAX, RIA and Web services are three important technological vectors for the WEB 2.0 application space. With these new technologies come new security issues, and ignoring them can lead to big disasters for the corporate world. However, that said, while Web 2.0 may present different types of challenges, those are not necessarily any worse than the risks involved with legacy applications - they're just different. And the opportunities that Web 2.0 technology can provide a business make overcoming these potential threats worth the effort.