Web of Discoveries: Journal of Analysis and Inventions
webofjournals.com/index.php/3

CLASSIFICATION OF THREATS TO WEBSITES BY LEVELS

Anvarjon Abdujabborovich Mahkamov
International Islamic Academy of Uzbekistan, Senior Teacher of the
"Department of Modern ICT", A.Kadiri, Tashkent, 100011, Uzbekistan
mahkamovanvar2020@gmail.com 11

Abstract
This article provides a brief overview of the classification of threats to websites by level. The above information helps us to closely study the threats to websites. The user can anticipate and control threats to websites. It detects and eliminates illegal activities, harmful situations and certain types of risks.

Keywords: web sites, threats, classification of levels, security.

Introduction

Today, the importance of information in the life of any developed society is constantly increasing. From a long time ago, the information of the military-strategic importance of the state was strictly kept secret and protected. Information technologies are constantly improving in the areas of automation and information protection. Not everyone understands how it is possible to lose information and what the consequences are. For example, hackers have caused significant damage to companies such as Yahoo.com, Amazon.com, and even NASA, the space exploration agency. RSA Security, one of the biggest players in the security services market, has come under attack just days after it recklessly announced that it had measures in place against any threat[1, 2].

Threats to information security can take many forms. The most serious threats for 2018 were "Crime-as-a-Service", threats related to Internet products, supply chains and the complexity of regulatory requirements. "Service crimes" is an example of a darknet marketplace for large criminal communities offering a package of criminal services at low cost to emerging cybercriminals. This enables hacking attacks that were previously unattainable due to high technical complexity or high cost.

This makes cybercrime a mass phenomenon. Many organizations are actively implementing Internet products. These devices are often designed without security requirements in mind, creating additional opportunities for cyberattacks.

In addition, it is difficult for organizations themselves to monitor which of the data collected by lot devices is transferred[1, 4].

The threat to supply chains is that organizations share a variety of valuable and sensitive information with their suppliers, resulting in a loss of direct control over them.

Thus, the risk of compromising the confidentiality, integrity or availability of this information is greatly increased. Although simplifying the processing of personal data implies improvement of information security in the long term, the risks of organizations increase significantly in the short term. If there is any weakness in the provision of information security, threats can be carried out by users.

Web of Discoveries: Journal of Analysis and Inventions
webofjournals.com/index.php/3

As a result of these threats, it is possible to cause great damage to the national economy network. The table below shows some of the possible threats[3, 5].

Table 1: Threat types and entities

T/R	Types of threats	Operator	Chief	Programmer	engineer (technician)	Beneficiary	Competitor
1	**Change codes**	+		+			
2	**Move files**	+		+			
3	**Delete files**	+	+	+		+	+
4	**Mastering programs**			+	+		+
5	**Espionage**	+	+	+			+
6	**Secret surveillance**			+	+		+
7	**Sabotage**	+		+	+		+
8	**Selling data**	+	+	+		+	+
9	**Theft**		+	+		+	+

Cyber-attacks against public websites are very common today, regardless of size, origin and classification, and in most cases, such attacks cause the following problems:

- Tampering with the website;
- Hiding the existence of the website and creating a denial of service (DoS) situation;
- Tampering or falsifying the names of confidential clients and organizations;
- The attacker takes control of the entire site or uses the website as the main weapon to carry out attacks;

All of these attacks have a significant impact on the principles of information security, destroying the concepts of integrity, confidentiality and usability, which are considered to be the main characteristics of information security.

In general, protecting not only a website, but any object in the field of information security requires a comprehensive conceptual level approach[6].

Security measures may vary depending on the type of website, but in general, for the security of any website, we need to pay particular attention to the following processes.

Secure Domain Ecosystem - The internet as we know it is directly dependent on DNS (Domain Name System). It's like the Internet's phone book, domain names are translated into IP addresses, so a site user can easily find a website by typing its name instead of a string of numbers.

Web of Discoveries: Journal of Analysis and Inventions
webofjournals.com/index.php/3

DNS is not a single entity, it includes a protocol, a namespace, and a service. DNS security is the practice of protecting the DNS infrastructure from cyber attacks to keep it running fast and reliably. An effective DNS security strategy includes a number of overlapping safeguards, including deploying redundant DNS servers, implementing security protocols such as DNSSEC, and requiring strict DNS logging [3, 4].

Secure User Accounts - Careful use of user accounts is the most important form of security for your network.

Properly configured user accounts prevent unauthorized users from accessing the network even if they have physical access to the network.

Secure data in transit - Hypertext Transfer Protocol Secure (HTTPS) and HTTP Strict Transport Security (HSTS) will be used instead of Hypertext Transfer Protocol (HTTP). HTTPS ensures that data is transmitted in an encrypted state through the network protocol and cannot be read by unauthorized persons.

Data Backup - By automatically backing up important website data and website settings, you can keep your data safe and secure.

Secure web servers - The server supports a security protocol such as SSL.

Order forms with credit card numbers and other confidential information transmitted from the web server must be encrypted for user protection. Even if a third party were to intercept the transmission, it would be very difficult to encrypt the data.

OpenID is a technology that offers access to multiple websites using an existing account without generating a new password.

People register on various websites and have many accounts in their daily life, but remembering or saving the password for all of them can cause a lot of inconvenience to users.

In such situations, OpenID offers its own solution to this problem. With OpenID, you only need one username and password.

With an identity provider, one can create an account with an ID and password, and this provider authenticates the user's identity to the websites visited. No other website can see the password except the provider.

OpenID was officially introduced in 2005. Many large enterprises use OpenID, including Google, Facebook, Yahoo!, Microsoft, AOL, MySpace, Sears, Universal Music Group, France Telecom, Novell, Sun, Telecom Italia[6].

The user has his own account with the OpenID provider and must introduce his identity to the system with his personal ID. An OpenID can be an identifier or a URL.

By using this OpenID user can access any website.

The authentication process can be done using OpenID, because every user can be identified using OpenID.

A user who has an account registered with an OpenID provider will need to provide their information when accessing any website.

When a user enters their OpenID into the system, the system forwards this unique password log to the OpenID provider. Then the user will need to authenticate himself at the OpenID provider.

Figure 1 below shows an example of Jenkins prompting a user to enter their OpenID.

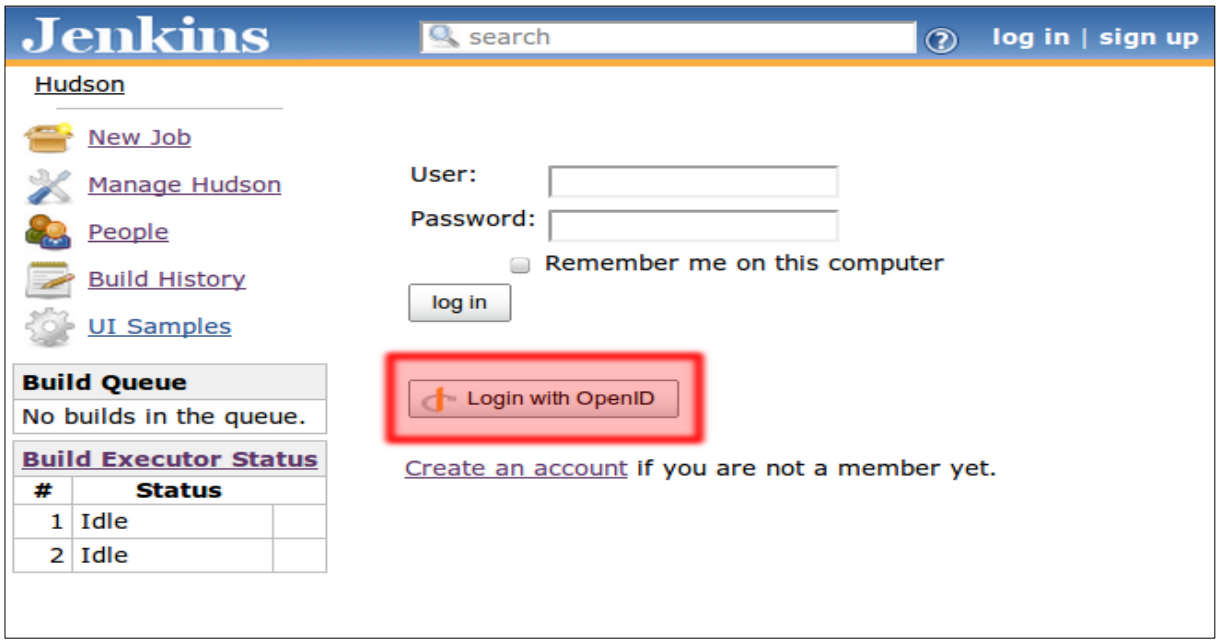

Figure 1. Login with OpenID in Jenkins

After the user successfully authenticates, the OpenID provider forwards the user's identity to the system. The system then allows the user to access their website.

Conclusion

In conclusion, the above methods will help us to control the processes in the network, to analyze suspicious files and to neutralize the files that are placed by various filters.

References

1. Zhumaev, T.S., Mirzaev, N.S., & Makhkamov, A.S. (2015). Algorithms for segmentation of color images based on the selection of strongly coupled elements. Studies of Technical Sciences,(4), 22(27),

2. Маҳкамов, А. А., & Инадуллаев, Х.Ў.Ў. (2021). Сравнительный анализ биометрических систем в обеспечении информационной безопасности. Universum: технические науки, (12-1 (93)), 32-37.

3. Махкамов А. А. Алгоритмы идентификации личности человека по изображению ушных раковин //Исследования технических наук. – 2015. – №. 4. – С. 28-32.

4. Boyens, C., G¨unther, O.: Trust Is not Enough: Privacy and Security in ASP and Web Service Environments. In: Sixth East-European Conference on Advances in Databases and Information Systems. Volume 2435 of Lecture Notes In Computer Science. (2002) .

5. R. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E. Youman, "Role-Based Access Control Models," Computer, vol. 29, no. 2, pp. 38-47, 1996.

6. MySQL ma'lumotlar bazasi haqida https://www.postgresql.org/about/

Web of Discoveries: Journal of Analysis and Inventions
webofjournals.com/index.php/3