


Computer science → Fundamentals → Essentials → Security

Web security, OWASP

Theory

Practice

 0% completed, 0 problems solved

▼

Theory

🕒 7 minutes reading

Verify to skip

Start practicing

Everyone uses the Internet: from regular people using social networks and watching movies to serious developers creating various websites. What all these people have in common is that their data is stored on the network and can be accessed if it is not secure. For data protection, there is a concept of web security.

In this topic we will take a closer look at what web security is, why we should monitor security, what types of vulnerabilities exist, and how we can find them.

§1. What is web security

Web security is a set of measures and protocols aimed at protecting data from viruses, spam, and other threats that can harm a website, application, and/or specific user's data. It encompasses Internet, browser security, website security, and network security as it applies to other applications or operating systems as a whole.



The main idea of web security is that the Internet is an inherently insecure channel for information exchange. This idea is reflected in two key concepts:


- No one is ever 100% safe. Any site or account may be hacked. There is no notion of being 100% protected from this.
- One layer of security is not enough. For example, a password from a social network or website is a good idea, but it alone may not be enough. Therefore, after entering a username and password, additional means of user authentication like one-time PINs are often required.

There are different types of threats both ordinary users and developers can face so let's review the main ones.


§2. Threats

Generally, users face the following threats:

1 required topic

  World Wide Web ▼

2 dependent topics

 Getting started with Spring Security ▼

Cross-site scripting ▼

- **Malware** such as viruses or Trojans. An Internet user can be tricked into downloading malicious software onto a computer. Antiviruses help avoid them.
- **Dos attack** is a type of hacker attack on a system in which real users receive a denial of service.
- **Phishing** is a type of online fraud in which attackers gain access to confidential user information such as username and password. In order to reduce the likelihood of such an attack, two-step user authentication is used. Passwords can also be changed periodically.
- **Application vulnerabilities.** If a site or program can be hacked, then it has a weak point, which is called a vulnerability. Vulnerabilities are different, they have their own classification and types.

We will discuss the last threat type in more detail below.

§3. Security vulnerabilities

Web security vulnerabilities are prioritized depending on exploitability, detectability, and impact on software.

- **Exploitability** is what hackers should do to exploit the security vulnerability. The high exploitability is when an attacker needs only a web browser, and the low one is when an attacker needs advanced programming and tools.
- **Detectability** answers the question of how easy it is to detect the threat. It is easy to detect if the information is displayed in the URL or error message. In this case, we get the highest detectability level. And if it is in the source code, then it is much more difficult to find. Then the level of detectability will be very low.
- **Impact or Damage** stands for the amount of damage that will be done if the security vulnerability is exposed or attacked. The highest impact will cause a complete system crash and the lowest one does nothing at all.

There are many risks and weaknesses that may lead to vulnerabilities, the most frequent ones can be found in the [OWASP TOP-10 rating](#), which is updated every three to four years. We left the link above for the 2021 ranking. **OWASP** stands for an **Open Web Application Security Project**, an online community that publishes articles on the topic of web application security, as well as documentation, various tools, and technologies. With the help of their TOP-10 list, users can be aware of the most critical risks and threats, their consequences, and countermeasures.

Despite all of the above, it is not always possible to foresee all the weak points of a site or a program. It often happens that companies hire people who specifically attack their products in order to find vulnerabilities. This is done using a special Bug Bounty program.

§4. Bug Bounty

A **Bug Bounty** program is a deal offered by many websites, organizations, and software developers. Through it, people can be recognized and rewarded for finding bugs, especially those related to vulnerabilities. With these programs developers can detect and fix bugs before the general public knows about them, preventing hacking. In particular, Bug Bounty programs have been implemented by Facebook, Yahoo!, Google, Apple, Microsoft, etc.

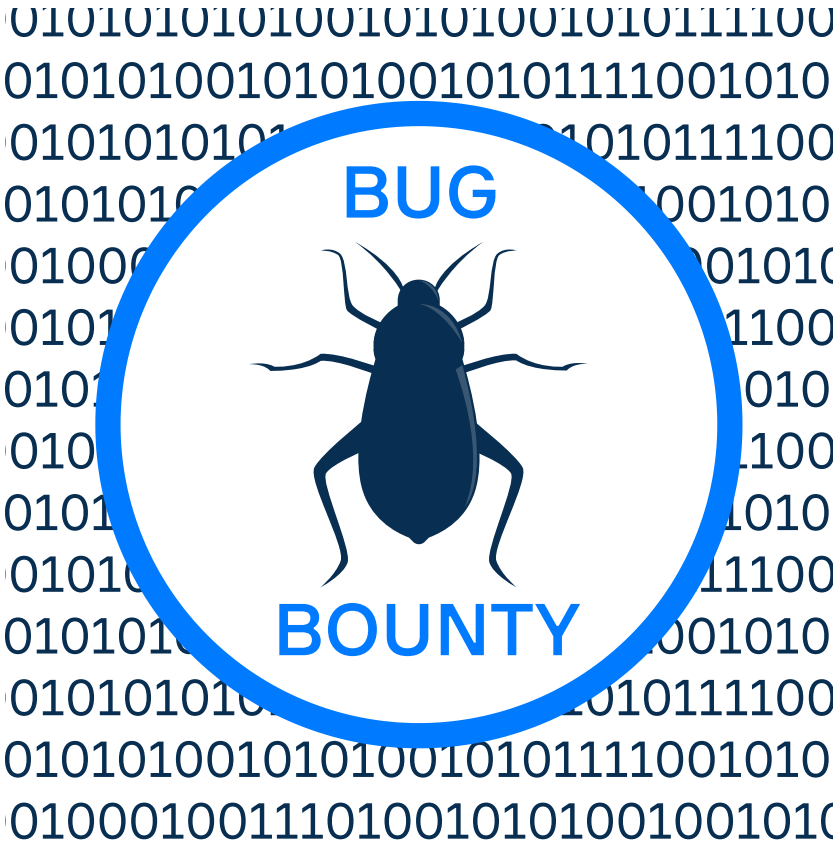
Table of contents:

[1 Web security, OWASP](#)

[§1. What is web security.](#)

[§2. Threats](#)

[§3. Security vulnerabilities](#)



[§4. Bug Bounty.](#)

[§5. Conclusion](#)

[Discussion](#)

In general, they work like this: the company establishes the rules indicating what exactly one can try to break and get a reward for. These can be new features in the application, functional updates, integration with other services. As soon as changes take place, there is a chance of error. Then users begin to investigate these updates.

This approach gives the company the ability to constantly test its product and always know where a problem might arise. People find bugs, and then developers fix them.

§5. Conclusion

To sum up,

- **web security** is a set of measures and protocols aimed at protecting data from viruses, spam, and other threats
- the main threats are **malware**, **dos attacks**, **phishing**, and **application vulnerabilities**
- the most frequent vulnerabilities can be found in the **OWASP TOP-10** rating
- companies can hire people to search for vulnerabilities using the **Bug Bounty** program.

[Report a typo](#)

85 users liked this piece of theory. 1 didn't like it. **What about you?**



Start practicing

[Verify to skip](#)

[Comments \(3\)](#)

[Useful links \(0\)](#)

[Show discussion](#)

