УДК 004.056:004.774

INFORMATION SECURITY OF WEB APPLICATIONS

Ivanov A.P.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Perevyshko A.I. – lecturer of the department of foreign languages

Annotation: This article is devoted to the information security of web applications. The main types of attacks and vulnerabilities are considered. The main methods and conditions for countering such attacks are emphasized.

Keywords: web application, XSS vulnerability, DoS attacks, CSRF attacks, SQL injection, security, data, analysis.

Introduction. Due to the active use of the Internet, people have started to use web applications, but today's applications exist in a completely different environment compared to those in the beginning. There are many hackers in the world who are willing to get their hands on any in-formation for a certain reward, thus the problem of leaking information from these sources arises. Most of the applications contain important information which is not to be disclosed, hence it is necessary to secure these applications from the very beginning, hence some security tasks should be done. In this paper, we will consider the types of vulnerabilities, their types and ways to protect against them.

Main part. Most web applications are written in different programming languages such as HTML, Java, CSS, PHP, jQuery. Since all programming languages have different structure, respectively these programs have different vulnerabilities and ways of protection. In order to fully protect your application, you need to act according to a certain plan, which is presented below in figure 1:

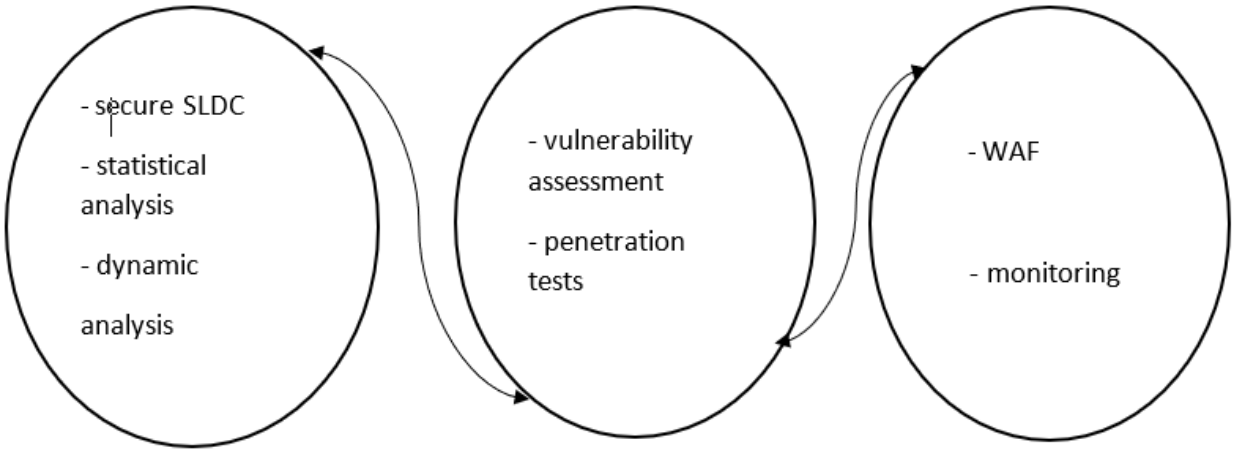

Figure 1 – Secure development, secure deployment, secure use

Now let's look more specifically at each step:

1. Safe development. At this stage, we need to carry out static and dynamic analysis. Statistical analysis is a tool ('white box') which scans errors of source code. Dynamic analysis is a tool ('black box') which scans errors of the launched application.

2. Secure deployment. Vulnerability assessment and penetration tests are performed as early as stage. Vulnerability assessment – the application is scanned with or without an account. Penetration test - hacking of this application in order to identify weaknesses that need to be protected.

3. Safe use. At this stage, the main emphasis is placed on WAF, which scans the application and detects any errors. WAF is a network tool which monitors traffic to the web application.

One of the most popular and widespread vulnerabilities is XSS (cross-site scripting) – a vulnerability resulting from insufficient filtering of data sent to malicious users and its subsequent

output to third parties. There are 3 main types of XSS attacks: stored, reflected, via DOM. Let's take a look at one of these types, stored XSS, which is the most common type.

To counter such an attack, it is necessary to use expression, forbidden script tags, and CSPs. At the moment, these vulnerabilities have become less common, but XSS has been around practically since the advent of the Internet, and the essence of this attack is not changing, but increasing the area of application.

At the moment, the most publicized type of attack is DoS-attacks. DoS-distributed of service, which means denial of service. In this attack, a large number of devices fill the server of any application with requests, and the application begins to slow down its work. There are varieties of this attack, an example is ReDoS-attack and distributed DoS-attack. These attacks use certain code flaws and bugs in it, just the part where regular expressions and actions are used. Since this type of attack is considered massive, the application servers are overflowing with requests from malicious users, thereby ordinary users can’t get an answer to their request.

To summarize this attack, they only cause the lack of functionality of the application for a certain period of time. But it should be taken into account that data leakage is possible, so be sure to follow the application code and errors, after such attacks, in order to fix them.

In addition to attacks, there are injections, that is, changing any part of the code. The most common is SQL injection. To detect such an injection is required to make a list of all the parameters that can handle the program, and should check the values of fields HTTP-header. By doing so, you can notice some embedded in the code of the program lines and parts of the code should be replaced by non-integer values, specified in quotation marks. In fact, these errors are among the most common, but to prevent them, you should follow a couple of simple and elementary rules.

As the world is improving, respectively, and improving themselves web-applications, that is, the surface and methods of attack significantly increase every year. Having analyzed all the vulnerabilities and attacks, we can conclude that the main reason for the appearance of such problems is that any user can interfere with the interaction between the browser and web-application server. Thus, data that is false and derived from unofficial sources cannot be trusted.

To prevent the attacks and vulnerabilities described above, you should use modern and innovative methods of writing code. The Cryptography Service Provider (CSP) can also be used. To reduce the risk of an attack, HTTP requests should not be able to change the code or composition of the application. Web application requests should be verified by middleware which helps in reducing the risk and probability of such an attack. The system log of the application must be maintained, which means that the application must have a user registration system and log all requests sent by them. It must be specified in the application code that the user cannot 'grab' resources for any long period of time.

Conclusion. To ensure the safe operation of any web-application should follow a couple of simple rules and in some situations think like an intruder. In order to prevent attacks that are intended by the intruder. This report does not cover all possible attacks and vulnerabilities, but the most important and popular ones that are common in our world. I hope you learned a lot and would be very happy if this report is useful in protecting your application.

References

1. BHV Publishing House-Petersburg, Tactics of protection and attacks on Web applications / BHV Publishing House-Petersburg - 2005. - 432c.

2. Andrew Hoffaman, Web application Security / Andrew Hoffaman - 2021– - 336c.

3. AK Kamal Security, WEB applications building a security program / AK Kamal Security - 2020.- 32c.

4. Georgia Weidman, Penetration Testing / Georgia Weidman - 2014. - 531c.