WEB OF SCIENTIST: INTERNATIONAL SCIENTIFIC RESEARCH JOURNAL
ISSN: 2776-0979, Volume 3, Issue 5, May., 2022

SECURITY OF SITES AND WEB APPS

Salikhova Venera Karimdzhanovna
Lecturer in the Department of Mathematics and General Economics at TSUOS

Annotation
The article describes the most common types of attacks and various vulnerabilities with which hackers manage to penetrate and hack a software product. The relevance of this topic is due to the fact that, despite the high progress in the field of system security, many systems, including websites, can still be hacked by intruders.

Keywords: Vulnerability, security, information security, Dos-attack server.

Introduction

One of the most important aspects of website security is keeping your customer information safe. If your website collects any personal information or PPI, this is doubled. What is PPI? Often he gets credit card numbers, social security numbers, and even address information. You must withhold this confidential information from your client during receipt and distribution. You must provide this information as soon as you receive it, regarding how you will use and store it in the future.

A final note about protecting customer data. Remember that SSL only encrypts files during transfer. Once you get to your company, you are responsible for this information. How customer data is processed and stored is just as important as data security. This may sound crazy, but I have actually seen companies where customers print out order information and keep paper copies of the files when problems arise. This is a clear violation of security protocols, and depending on the state you work in, you can be fined large sums of money for such violations, especially if these files end up being corrupted. It makes no sense to protect the data in transit, but then delete the data and save it in a safe place!

Most modern information systems are created in the form of Web sites, so security must be given special attention. As soon as a device appears with an operating system and a software application, it immediately attracts the interest of intruders. They begin to study it and hack it. In the last year, this trend has been the subject of many reports at major hacker conferences. Developers do not always pay special attention to the complete protection and security of the created sites, although it plays a very important role, because each site can be hacked in one way or another, given that sites can be very diverse : electronic libraries, social networks, Web portals of various

educational institutions, online stores, official sites of various organizations, banks, and so on.

First of all, you need to pay attention to the security of the web server, since it is he who is responsible for receiving and processing HTTP requests from clients to the website. It is he who ensures the functioning of numerous websites around the world, and is also responsible for basic services and stores personal data of both users and site visitors. The need to protect servers is one of the most important tasks of any organization.

Even during the appearance of the first Web sites, hackers carried out attacks on the sites of important organizations, such as the American CitiBank (1994), as a result of which 12 million dollars were stolen, and the sites of NATO, the CIA, and the Ministry of Justice also became victims. USA. At present, it would seem that such threats should become much less or not exist at all, but, alas, this is far from being the case: as before, a fairly large number of cyber attacks are now being carried out, and mainly on such global organizations as government agencies and banks. This is due to the fact that it is not possible to receive / change information that can somehow affect important events for the state.

A rather important point is that the geographical location of the server does not affect its protection in any way. You can attack it from any access point. This is due to the fact that Web servers, by virtue of their openness, are designed to transfer information between users and that is why they have many vulnerabilities. For example, an attacker can make some changes (modifications) to the code of the HTTP server or database server, or the website pages themselves, changing its original functionality.

Website Protection helps protect your website from:

DDoS Attacks

This is a malicious attack that disrupts the normal operation of a website. It does this by flooding the website's surrounding infrastructure with unnecessary internet traffic.

Malware:

Used to spread spam, steal confidential customer information, and gain unauthorized access to the site.

Blacklis

This results in the unauthorized removal of a website from search results. It may also include warning labels that will deter visitors.

Drawback

Replaces website content with malicious content.

Exploiting Weaknesses

Exploiting vulnerabilities in a website, such as old plugins, to gain control of a website. Given that hacking threatens the internet by exploiting website security vulnerabilities through automated scripts, here are 12 top tips to help keep your website secure online.

- Update your software regularly
- Use HTTPS
- Search for SQL injections
- Invest in automatic backups
- Installing a Web Application Wall (WAF)
- Strengthen access control
- Hide admin pages
- Restrict file uploads
- Check your email transfer ports
- Protect yourself from XSS attacks
- Simplify error messages
- Install website vulnerability scanners

Remember, you can't reduce existing risks to absolute zero, but these simple steps are necessary to keep your site as secure as possible.

Bibliography

1. Chris Mitchell. Artem Konev. Website security. // Australia: SophosLabs. [Electronic resource]. URL: http://help.yandex.ru/webmaster/protecting-sites/contents.xml (accessed 02/15/2016).
2. Smirnov S.N. Security of database systems - M .: Helios ARV, 2007.-352s., Ill.
3. Kaspersky Lab: Sophisticated cyberattacks have replaced mass epidemics [Electronic resource].
   URL: http://pda.cnews.ru/reviews/index.shtml?2014/12/24/591211 (date of access: 02/15/2016)
4. Biryukov A.A. Information security: defense and attack - M.: DMK Press, 2012.-474.: ill.