Discuss IFrame Injection Attacks

The type of attack technique IFrame Injection is still the most basic and popular form of cross-site scripting - XSS model .

By inserting dynamic websites (ASP, PHP, CGI, JSP .) HTML tags or dangerous script code, in which the dangerous code inserted is mostly written with Client-Site Script like JavaScript , JScript, DHTML and also basic HTML tags. If you find that someone is targeting your website with this technique, don't worry too much. Here are some things to do when the website falls into this situation.

For example, a malicious code is often used to attack:

```
{xtypo_code}
iframe src="http://www.example-hacker-site.com/inject/some-parameters" width="1" height="1"
frameborder="0"
content of malicious code
{/ xtypo_code}
```

1. Regularly maintain the website in a certain period of time:

Security experts recommend that administrators remove the entire website to avoid becoming the focus of spreading malicious code. And during the entire recovery process, continue to keep the offline status of the website.

2. Change all passwords:

At first glance it seems simple, many administrators seem to be not paying attention to this extremely important step. After being peeked at by hackers, you should renew all passwords including ftp, ssh accounts, admin accounts, databases .

3. Save 1 copy of the website for analysis:

To determine which causes and weaknesses have been exploited by hackers, you need to keep a copy of the original status at the time of the attack. This is very useful for analyzing and preventing future threats, you should save the website as a compressed file in rar, zip or gzip format and store in a safe place. Note that this quarantine file should never be saved directly on the server.

4. Replace the entire website with a completely clean backup:

Do not rely too much on host providers that will back up all your data. A lot of tech support regularly asserts that they have scheduled automatic backups, but nothing can be as certain as what you do on your own, moreover,

two backup options are always better. 1 option

5. Check the website and upload it again:

This process should be thoughtful to ensure that the entire website is safe and error free, then you can post it again as before.

6. Learn about the origin of the attacks:

To ensure that the attacks will never be repeated, administrators should conduct a complete, detailed analysis and analysis of the attack. Where is the error? Security vulnerabilities or web applications? Or due to the decentralized decentralized mode, confused? Can the website be infected directly from the server hosting the data? All must be thoroughly researched and analyzed. If necessary, ask security experts from leading security companies such as Kaspersky, BitDefender, Norton, Panda, Avira .

7. Apply appropriate security measures:

Although you have successfully restored the website, there is no guarantee that your website will not be attacked again. If the old security vulnerability has not been overcome, it is possible that your website will be paralyzed tonight. Based on the analysis results obtained in the previous step, you should apply appropriate security measures, upgrade the server, install additional security programs, upgrade the entire web application or use the rules Completely new privacy laws.

Based on management experience and information gathered, we can contribute some more advice and objective predictions about the causes as follows.

Easy causes:

1. Website using cheap host service
2. Based on the old version of open source applications, such as WordPress 1.0 . which has many holes
3. Data access on the server is set in no particular order, for example, the right to manipulate data at 777 level - read, write and execute
4. Shortcomings of application software
5. Use FTP instead of SFTP
6. Unlimited IP for SSH and FTP accounts

Some simple but useful operations:

1. Change your password periodically, for example, every 2 weeks or 4 weeks
2. Always update the stable version of the application
3. Regularly 'clean up' the data folder on the server, notice if strange files suddenly appear
4. Decentralization levels are set correctly
5. Frequently communicate with units and experts to provide security services to receive the best advice.