What is Reflected XSS? How to know if you are attacked by Reflected XSS

Reflected XSS is a type of cross-site scripting attack. Hackers insert malicious JavaScript code into a web page and then trick visitors into clicking on a link containing the malicious code.

One of the most common forms of cross-site scripting attacks today is Reflected XSS. This is a very dangerous form of attack because even if only one out of 1,000 email recipients clicks on the link, dozens of other users are still infected. So what is Reflected XSS and how to detect it? Let's find out with ***TipsMake*** in the following article.

What is Reflected XSS?

Reflected XSS is a type of cross-site scripting attack. Hackers will insert malicious JavaScript code into a website and then trick viewers into clicking on a link containing the malicious code. When users click on the link containing this malicious code, the code will be executed in their browser without being stored on the server. From there, the bad guys can access sensitive information such as cookies, session IDs, .

What is Reflected XSS?

Targets of Reflected XSS attacks

Reflected XSS attacks are performed for the following purposes:

1. Stealing user information: Attackers can steal cookies or session tokens, thereby taking control of the victim's account on the websites they are using.
2. Perform unwanted actions: Once taken over, the attacker can perform actions such as sending fake messages, changing account information, or even spreading malware to other users.
3. Browser Control: Malicious code executed in the victim's browser is a tool for attackers to modify, control the user interface or collect additional data from users without their knowledge.
4. Spreading malware: Attackers can use Reflected XSS to spread malware to other computers, creating a network of infected devices.

How is Reflected XSS implemented?

The Reflected XSS implementation process is similar to other forms of cross-site scripting attacks, including the following four main steps:

1. **Step 1:** The attacker creates a URL containing malicious code, usually JavaScript. For example: http://example.com/search?query=
2. **Step 2:** The attacker sends a malicious link via email, social media, or other means to trick the victim into clicking on it.
3. **Step 3:** When the victim clicks on the link, their browser sends a request to the server with the parameters in the URL. If the web application does not validate and handle the input safely, it will respond with the injected malicious code.
4. **Step 4:** The malicious code responded from the server will be executed in the victim's browser environment.

How to check Reflected XSS

Use automated tools

There are many automated tools available today that can help detect Reflected XSS vulnerabilities, such as Burp Suite, OWASP ZAP, and Acunetix. These tools are capable of scanning and analyzing a website's input parameters to determine if they are vulnerable to XSS.

When using these tools, you simply enter a URL and the tool will automatically perform the tests. If a vulnerability is found, the tool will provide detailed information on how to fix it.

Perform manual testing

In addition to using automated tools, it is also important to perform manual testing. Security personnel can test URL parameters by inserting JavaScript code to see if the code is executed.

For example, you can experiment with input parameters like:

http://example.com/search?q=alert('XSS')

If when you click on this link and see a warning window appear, this indicates that the website may be vulnerable to Reflected XSS.

Check all data entry points

One way to check if you are vulnerable to Reflected XSS is to examine each entry point in your application's HTTP requests individually. An entry point is any data in a URL query string, file path, or message body, including parameters and HTTP headers. However, it can be more difficult to exploit HTTP headers for XSS attacks.

Use random values

Try sending unique, random alphanumeric values ??to each data entry point to test whether the response reflects the values. These values ??should be short and simple enough to pass most input validation, containing only letters and numbers. They should also have enough characters to reduce the chance of a random match, so values ??around eight characters work best.

Conclude

From stealing personal information to conducting phishing attacks, Reflected XSS is a serious threat that everyone needs to pay attention to, especially businesses. Hopefully, through this article of TipsMake, readers have learned more about a popular form of cross-site scripting attack today.

You finished reading the article "**What is Reflected XSS? How to know if you are attacked by Reflected XSS** " edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.