

Forum:[Hack Forums](#)

Thread: [Explain Unvalidated Redirects and apply them to the Kaspersky Web site](#)

Mr8n - November 4, 2018, 10:11 pm

Before I begin to explain the Unvalidated Redirects gaps

Let us give a simple example to understand the idea of Redirection

The user receives a message on his e-mail with the following content:

Dear user .. You can visit our blog through the following link:

<http://www.goodsite.com/link.php?url=http://blog.goodsite.com>

If the user clicks the link above, they will be directed to <http://blog.goodsite.com>

So how can the link above be exploited?

It is very simple. The hacker will replace the link to which the user will be redirected to another link until the user is redirected to the attacker's site.

Example:

Dear user .. You can visit our blog through the following link:

<http://www.goodsite.com/link.php?url=http://blog.attacker.com>

If the user clicks the link above, they will be directed to <http://blog.attacker.com>

However, as you can see, the user has been redirected through the site of goodsite.com, which is supposed to be a trusted site for users.

What is the risk to the user through this type of gap?

1. Converting the user to fake login pages similar to the same login page for the original site and the domain name may also be similar to the same domain name as the original site and thus steal the user's login data.

Example: Instead of being transferred to Facebook, www.facebook.com you are redirected to www.faecbook.com Have you noticed the difference?

2. Download of malicious files (Trojans) on the devices of users .. An attacker can turn the user on the page exploits a gap in the software installed on the user's device .. Software such as Java, Flash Player, Adobe Reader and others

What is the cause of this vulnerability? How does the programmer protect himself from them?

The error is that the programmer does not use any type of validation to verify the link to which the user will be redirected!

Some ways to protect against this vulnerability:

1. Security Tokens

What are Security Tokens?

Are numbers that are configured with some type of encryption (according to the programmer). For example, they are aggregated from the link of the site + current time + Salt

Example:

"TRIfZRIE_yke-3Z1pFaHaDC5FOPEXEGx6LpRZdjW"

The link becomes as follows:

http://www.goodsite.com/link.php?url=http://blog.goodsite.com&token=TRIfZRIE_yke-3Z1pFaHaDC5FOPEXEGx6LpRZdjW

If the Token function in this case is to make sure that the link to which the user will be transferred is a trusted link and registered in the site database and not manipulated because each link has only one Security Token.

2. Black & White List

Where the programmer creates a list of trusted sites to which users are converted to and except those sites, the user is not converted to anything else, but a page appears in error if the site is being manipulated to which the user is converted.

We come here for a practical example on the site of the company Kaspersky giant software companies to produce information security .. The site was infected with a gap of the kind we are talking today

In the next video we find that the gap was exploited in simulation to simulate the exploitation of the vulnerability by the hackers and used in the deployment of malicious files (Trojans) taking advantage of the name and trust Kaspersky users.

Imagine with me Dear Link comes to you from Kaspersky (which is a reliable source not an instant) and asks you to upload a file! Or a page you are transferred from the site of Kaspersky and ask you for certain data or download the latest version of Kaspersky and paid for free!

"The most trusted source for you ... may be your worst enemy!"

The gap was discovered by the author of the subject and was reported to Kaspersky immediately after it was discovered and is currently being censored.

M L T - November 5, 2018, 12:53 am

Would have been cool if you'd listed some bypass methods and ways to further escalate impact. I'm soon going to do a tutorial on unvalidated redirects and forwards.