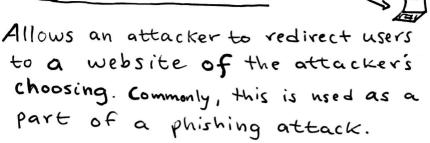
Open Redirection - -



Regular use cases:

- * Get a user back to a page after Logging in.
- * Pass single-sign on information to a third party.

https://vulnsite.com?next=/home

Once a user requests this URL, the Server will take the value of the "next" parameter to determine where to redirect the user (in this case, to the home page). HTTP/1.1 302 Found

Date: Wed, 16 Jun 2077: 22:10:48 GMT

Location: https://vulnsite.com/home

Connection: Close

Content - Type.text/html

Content - Length: 90

<html> <body> You are being

REDIRECTED

2/a> 2/body>
2/html>

"Location" header.

An HTTP response. Notice the

Now imagine that an attacker forms and submits this URL:

https://vulnsite.com?next=www.attacker.com

If the server does not validate the value of the "next parameter, then the HTTP response will be the following:

HTTP/I.1 Found

Date: Wed, 16 Jun 2077 22:10 GMT

Location: https://www.attacker.com

Connection: Close

Content-Type: text/html

Content length: 35

Lhtml> = body> You are being

La hvef='https://www.attacker.com'>

REDIRECTED

L/a> L/body>
L/html>

An attacker-controlled redirection.

The user will be seamlessly redirected to the attacker's web site.

Plan of Attack:

1. Attacker creates a malicious URL for the victim to click and sends it to them.

https://vulnsite.com?next=www.aHacker

2. The user clicks the link and is redirected to a malicious website.

<u>Dangers</u>: Attacker can abuse the trust of one site to get users to visit an evil site.

Remediation: Ensure that user-submitted URLs match an allowed value before redirecting Warn users that they are being redirected off-site to reduce

the Chance of a sucress ful phishing

attack.