Unvalidated Redirects and Forwards

OWASP Web App Top 10

SECURE CODE WARRIOR

What is it?

The “Unvalidated Redirect and Forwards” vulnerability allows trusted websites to be tricked into redirecting users to malicious websites, or forwards to be used to access unauthorized pages.

What causes it?

The problem is caused by using unvalidated parameters of a URL to determine the destination page of a user.

What could happen?

An attacker could use this vulnerability to redirect victims to malware or phishing sites. Credentials and other sensitive information could be stolen.
Additionally, forwards could be used to access unauthorized pages.

How to prevent it?

Avoid redirects and forwards unless absolutely necessary. If unavoidable then don’t use the user parameters as destination of the redirection/forward.

Unvalidated Redirects and Forwards

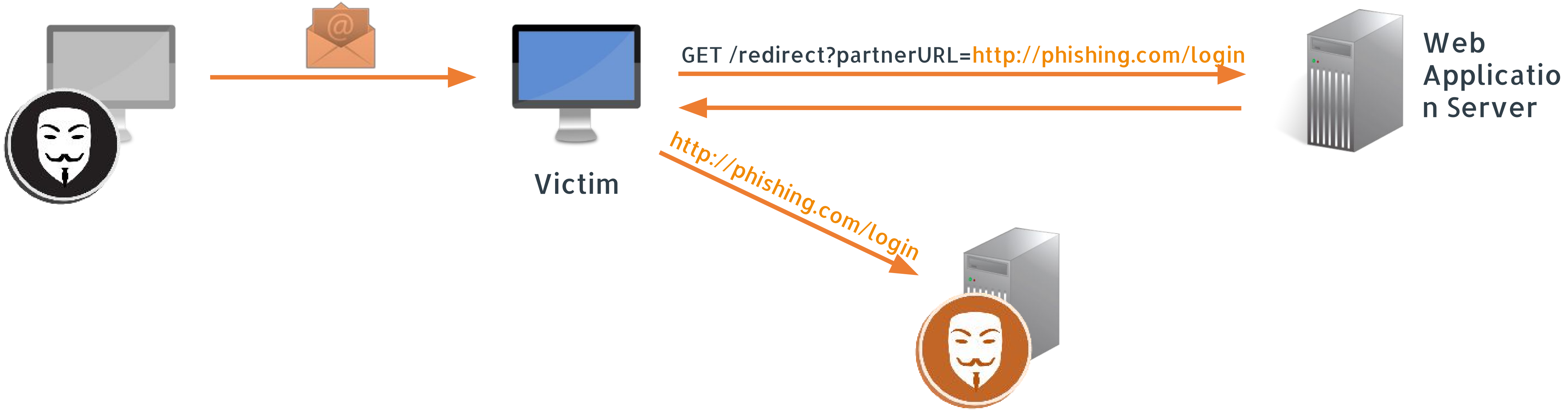
Understanding the security vulnerability

An attacker sends an e-mail to a victim. It contains a link to a vulnerable page with a redirect to a malicious site.

The user, trusting the root domain of the URL, clicks on the link.

The website does not validate the 'partnerURL' parameter and redirects the user to a phishing site.

The user is tricked into submitting the credentials of the trusted site. His account and personal information gets stolen.



GET /redirect?partnerURL=http://phishing.com/login
Web Applicatio n Server
Victim
http://phishing.com/login

Unvalidated Redirects and Forwards

Realizing the impact

Users could be redirected to malware or phishing sites, leading to loss of customer trust, reputational damage and financial loss.

Users disclosing sensitive information to phishing sites could lead to account theft, privacy violation and reputational damage.

Access to unauthorized administrative pages could lead to denial of service and financial damage.

Unvalidated Redirects and Forwards

Preventing the mistake

Avoid using redirects and forwards, if possible.

Don’t involve user input to determine the destination.

If parameters must be used, validate the supplied value and ensure it is authorized for the user.

Use mapping values rather than the actual URL’s.