Unvalidated Redirects and Forwards (A10)

Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

Threat agent:

Anyone who is sumbitting a request to your webpage.

Attack Vector:

Attacker links to unvalidated redirect and tricks victims into clicking it. Link is to a valid site, so the users are more likely to click on it. Unsafe forwarding to bypass security.

Security Weakness

Redirects and forwarders. Unvalidated parameter is used to choose the destination page. Detection is easy - check when you can set the full URL.

Technical impacts

Attempts to install malware or trick victims into disclosing passwords or other sensitive information.

Business impacts

Business value. Malware.

Am I Vulnerable to Forced Access?

Identify target URL with all the parameters. URL should contain only allowed and needed parameters.

Spider the web to see if it generates any redirects (HTTP.response.code 300-307)

How do I Prevent Forced Access?

Avoid redirects and forwards.

Don't involve user calculating the destination address. If you cannot avoid this, check if the supplied value is valid and authorized for the user

Example

URL redirects to malicious webpage, malware, and boom!

http://www.example.com/redirect.jsp?url=evil.com

If transaction is successful, user is sent to this webpage, for example. Attacker crafts a URL that will pass the application's access control check then forwards the attacker to an administrative function.

http://www.example.com/boring.jsp?fwd=admin.jsp