com/thoughtworks/go/server/GoServerLoadingIndicationHandler.java	62	2	SECURITY	UNVALIDATED_REDIRECT

The following redirection could be used by an attacker to redirect users to a phishing website.

Unvalidated redirects occur when an application redirects a user to a destination URL specified by a user supplied parameter that is not validated. Such vulnerabilities can be used to facilitate phishing attacks.

Scenario

1. A user is tricked into visiting the malicious URL:
http://website.com/login?redirect=http://evil.vvebsite.com/fake/login

2. The user is redirected to a fake login page that looks like a site they trust.
(http://evil.vvebsite.com/fake/login)

3. The user enters his credentials.

4. The evil site steals the user's credentials and redirects him to the original website.

This attack is plausible because most users don't double check the URL after the redirection. Also, redirection to an authentication page is very common.

Vulnerable Code:

protected void doGet(HttpServletRequest req, HttpServletResponse resp) throws ServletException, IOException { [...] resp.sendRedirect(req.getParameter("redirectUrl")); [...] }

Solution/Countermeasures:

Don't accept redirection destinations from users
Accept a destination key, and use it to look up the target (legal) destination
Accept only relative paths
White list URLs (if possible)
Validate that the beginning of the URL is part of a white list

References

WASC-38: URL Redirector Abuse
OWASP: Top 10 2013-A10: Unvalidated Redirects and Forwards
OWASP: Unvalidated Redirects and Forwards Cheat Sheet
CWE-601: URL Redirection to Untrusted Site ('Open Redirect')