U

URL Redirection Attack: Open Redirects, Warning Signs, and Prevention

A URL redirection attack sends users from a trusted-looking link to an unintended destination. Learn to identify redirect chains, respond safely, and prevent open redirects.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
6 min

CONTENTS

In this guide

01 Normal redirect vs malicious redirect
02 Common URL redirection attacks
03 Read the destination correctly
04 Signs of a malicious redirect
05 What to do after an unexpected redirect
06 How developers prevent open redirects
07 If your website redirects visitors unexpectedly
08 Frequently asked questions
09 References

A URL redirection attack sends a user from a trusted-looking link or website to an unintended destination. Redirection is a normal web feature used after sign-in, for shortened links, language selection, and moved pages. The security problem begins when an attacker controls the destination, compromises the redirecting page, or disguises where the chain ends.

An open redirect is one important form: a legitimate site accepts an untrusted destination parameter and redirects to it without adequate validation. Attackers can place that trusted domain at the beginning of a phishing link, bypass domain-based checks, or abuse the redirect inside an OAuth and authentication flow.

01 Normal redirect vs malicious redirect

Normal behavior	Suspicious behavior
A documented old page permanently moves to the publisher's new page	A trusted domain immediately forwards to an unrelated login or download site
A login returns to an internal page requested before authentication	A `returnUrl`, `next`, or `redirect` parameter accepts any external URL
A short-link service shows or allows verification of the final destination	The chain uses several unrelated domains to hide its endpoint
A regional redirect stays within the organization's verified domains	The destination uses a look-alike, newly registered, or misspelled domain
The user expected navigation	The redirect starts from an ad, compromised page, push notification, or extension without clear action

02 Common URL redirection attacks

- **Open redirect:** an application forwards to a user-controlled URL because destination input is not restricted.

- **Compromised-site redirect:** injected JavaScript, a malicious plugin, or changed server rules redirect selected visitors.
- **Malvertising chain:** an ad or intermediary sends users through tracking domains to scams, fake updates, or exploit pages.
- **Browser hijacking:** an extension, adware, proxy, or DNS change redirects searches and ordinary navigation.
- **Short-link abuse:** a shortened address conceals the final domain until the request is made.
- **OAuth redirect abuse:** weak callback validation leaks authorization codes or tokens to an attacker-controlled destination.
- **Phishing through a trusted domain:** a legitimate open-redirect URL increases credibility or bypasses message filters.

Not every unwanted redirect is an open-redirect vulnerability. A compromised website and an infected browser require different fixes, even though the user sees the same result.

03 Read the destination correctly

In `https://login.example.com.account-check.invalid/path`, the registered domain is under `invalid`, not `example.com`. Text before the final registered domain can be an arbitrary subdomain. Similarly, in a URL containing an `@` character, text before `@` may be user information rather than the destination host.

- Expand the address bar and find the actual hostname before entering credentials.
- Watch for Unicode look-alikes, extra words, hyphens, and misleading subdomains.
- Do not assume HTTPS means the site is legitimate; it only secures the connection to that host.
- Be cautious with percent-encoded or extremely long redirect parameters.
- When a message claims to link to an account, open the service through a saved bookmark or its known app instead.

04 Signs of a malicious redirect

- A familiar link ends on a different organization or domain.
- The page asks you to sign in again immediately after a redirect.
- A download, notification request, CAPTCHA, or browser-update prompt appears unexpectedly.
- Navigation passes through numerous domains or repeatedly returns to the same page.
- Only mobile users, search visitors, or first-time visitors are redirected.
- Searches redirect in several browsers or on every network.
- The destination asks you to paste a command, disable protection, or call a support number.

05 What to do after an unexpected redirect

1. **Do not enter information or download anything.** Close the destination tab.
2. **Open the intended service independently.** Use a verified bookmark, manually typed domain, or official app.
3. **Record the original link and final domain.** Preserve the message, screenshot, time, and redirect chain for reporting, but do not keep reopening it on a normal device.
4. **Check the browser.** Review extensions, notification permissions, home page, search provider, proxy, and DNS settings if redirects occur repeatedly.
5. **Scan the device.** This is especially important if a file ran, an extension was installed, or redirects affect unrelated sites.
6. **Protect accounts.** If credentials were entered, change the password from a clean device, revoke sessions, and enable MFA.
7. **Report the source.** Notify the organization whose domain or brand was abused and the service that delivered the link.

If redirects happen only on one website, the site itself may be compromised. If they occur in every browser on one device, investigate the device. If every device on one network is affected, check the router, DNS, and gateway.

06 How developers prevent open redirects

1. **Prefer relative internal paths.** If the application only needs to return users to its own pages, do not accept complete external URLs.
2. **Parse URLs with a maintained standard library.** Avoid handwritten string checks, simple prefixes, and blocklists that fail on encoding or hostname edge cases.
3. **Use a strict allowlist.** When external destinations are required, compare the parsed scheme, hostname, and port against exact approved values.
4. **Validate at the final redirect.** Do not trust a parameter merely because an earlier component checked it.
5. **Use destination identifiers.** Map a short server-side ID to a known URL instead of accepting an arbitrary address.
6. **Protect authentication flows.** Register exact OAuth redirect URIs, validate `state`, and follow the identity provider's current guidance.
7. **Show an interstitial for unavoidable external links.** Display the destination hostname and require a deliberate action.
8. **Log and test redirect behavior.** Detect new external destinations, encoded bypass attempts, and chains through your domain.

A check such as "URL starts with our domain" is unsafe because a malicious hostname can begin with trusted text. Compare the parsed hostname, not the raw string.

07 If your website redirects visitors unexpectedly

- Preserve web, DNS, CDN, plugin, deployment, and administrator logs.
- Check recently modified templates, scripts, server rules, tag-manager entries, and advertising code.
- Review administrator accounts, API keys, deployment tokens, and third-party integrations.
- Test different devices, referrers, user agents, regions, and clean sessions because malicious rules may target only some visitors.

- Remove injected code, patch the entry point, rotate exposed credentials, and invalidate caches.
- Request security-review or search-warning reconsideration only after verifying the site is clean.

08 Frequently asked questions

Is every shortened URL dangerous?

No. Shorteners are legitimate, but they hide the destination. Use preview features or open the claimed service independently when the link requests credentials or payment.

Can a redirect install malware automatically?

Most attacks still require a download, permission, or unpatched vulnerability. A malicious destination can attempt an exploit, so keep the browser updated and do not interact with unexpected prompts.

Does a VPN stop malicious redirects?

No. A VPN encrypts network traffic to its exit point; it does not validate redirect parameters, repair a compromised website, or remove a malicious extension.

09 References

- OWASP: Open Redirect
- OWASP Cheat Sheet: Unvalidated Redirects and Forwards
- Microsoft: Prevent open redirect attacks

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com