EXHIBIT 2

URL redirection

URL redirection, also called **URL forwarding**, is a World Wide Web technique for making a web page available under more than one URL address. When a web browser attempts to open a URL that has been redirected, a page with a different URL is opened. Similarly, domain redirection or domain forwarding is when all pages in a URL domain are redirected to a different domain, as when wikipedia.com and wikipedia.net are automatically redirected to wikipedia.org. URL redirection is done for various reasons: for URL shortening; to prevent broken links when web pages are moved; to allow multiple domain names belonging to the same owner to refer to a single web site; to guide navigation into and out of a website; for privacy protection; and for hostile purposes such as phishing attacks or malware distribution.

Contents

Purposes
- Similar domain names
- Moving pages to a new domain
- Logging outgoing links
- Short aliases for long URLs
- Meaningful, persistent aliases for long or changing URLs
- Post/Redirect/Get
- Device targeting and geotargeting
- Manipulating search engines
- Manipulating visitors
- Removing referer information

Implementation
- Manual redirect
- HTTP status codes 3xx
  - Redirect status codes and characteristics
  - Example HTTP response for a 301 redirect
  - Using server-side scripting for redirection
  - Apache HTTP Server mod_rewrite
  - nginx rewrite
- Refresh Meta tag and HTTP refresh header
- JavaScript redirects
- Frame redirects
- Redirect chains
- Redirect loops

Services
- URL redirection services
  - History
- Referrer masking

Security issues

See also

References

External links

Purposes

Similar domain names

A user might mistype a URL, for example, "example.com" and "exmaple.com". Organizations often register these "misspelled" domains and redirect them to the "correct" location: example.com. The addresses example.com and example.net could both redirect to a single domain, or web page, such as example.org. This technique is often used to "reserve" other top-level domains (TLD) with the same name, or make it easier for a true ".edu" or ".net" to redirect to a more recognizable ".com" domain.

Moving pages to a new domain

Web pages may be redirected to a new domain for three reasons:

- a site might desire, or need, to change its domain name;
- an author might move his or her individual pages to a new domain;
- two web sites might merge.

With URL redirects, incoming links to an outdated URL can be sent to the correct location. These links might be from other sites that have not realized that there is a change or from bookmarks/favorites that users have saved in their browsers. The same applies to search engines. They often have the older/outdated domain names and links in their database and will send search users to these old URLs. By using a "moved permanently" redirect to the new URL, visitors will still end up at the correct page. Also, in the next search engine pass, the search engine should detect and use the newer URL.

Logging outgoing links

The access logs of most web servers keep detailed information about where visitors came from and how they browsed the hosted site. They do not, however, log which links visitors left by. This is because the visitor's browser has no need to communicate with the original server when the visitor clicks on an outgoing link. This information can be captured in several ways. One way involves URL redirection. Instead of sending the visitor straight to the other site, links on the site can direct to a URL on the original website's domain that automatically redirects to the real target. This technique bears the downside of the delay caused by the additional request to the original website's server. As this added request will leave a trace in the server log, revealing exactly which link was followed, it can also be a privacy issue.[1] The same technique is also used by some corporate websites to implement a statement that the subsequent content is at another site, and therefore not necessarily affiliated with the corporation. In such scenarios, displaying the warning causes an additional delay

Short aliases for long URLs

Web applications often include lengthy descriptive attributes in their URLs which represent data hierarchies, command structures, transaction paths and session information. This practice results in a URL that is aesthetically unpleasant and difficult to remember, and which may not fit within the size limitations of microblogging sites. URL shortening services provide a solution to this problem by redirecting a user to a longer URL from a shorter one.

Meaningful, persistent aliases for long or changing URLs

Sometimes the URL of a page changes even though the content stays the same. Therefore, URL redirection can help users who have bookmarks. This is routinely done on Wikipedia whenever a page is renamed.

Post/Redirect/Get

Post/Redirect/Get (PRG) is a web development design pattern that prevents some duplicate form submissions, creating a more

Redirects can be effectively used for targeting purposes like geotargeting. Device targeting has become increasingly important with the rise of mobile clients. There are two approaches to serve mobile users: Make the website responsive or redirect to a mobile website version. If a mobile website version is offered, users with mobile clients will be automatically forwarded to the corresponding mobile content. For device targeting, client-side redirects or non-cacheable server-side redirects are used. Geotargeting is the approach to offer localized content and automatically forward the user to a localized version of the requested URL. This is helpful for websites that target audience in more than one location and/or language. Usually server-side redirects are used for Geotargeting but client-side redirects might be an option as well, depending on requirements.[2]

Manipulating search engines

Redirects have been used to manipulate search engines with unethical intentions, e.g. or URL hijacking. The goal of misleading redirects is to drive search traffic to landing pages, which do not have enough ranking power on their own or which are only remotely or not at all related to the search target. The approach requires a rank for a range of search terms with a number of URLs that would utilize sneaky redirects to forward the searcher to the target page. This method had a revival with the uprise of mobile devices and device targeting. URL hijacking is an off-domain redirect technique[3] that exploited the nature of the search engine's handling for temporary redirects. If a temporary redirect is encountered, search engines have to decide whether they assign the ranking value to the URL that initializes the redirect or to the redirect target URL. The URL that initiates the redirect may be kept to show up in search results, as the redirect indicates a temporary nature. Under certain circumstances it was possible to exploit this behaviour by applying temporary redirects to well-ranking URLs, leading to a replacement of the original URL in search results by the URL that initialized the redirect, therefore "stealing" the ranking. This method was usually combined with sneaky redirects to re-target the user stream from the search results to a target page. Search engines have developed efficient technologies to detect these kinds of manipulative approaches. Major search engines usually apply harsh ranking penalties on sites that get caught applying techniques lik these.[4]

Manipulating visitors

URL redirection is sometimes used as a part of phishing attacks that confuse visitors about which web site they are visiting.[5] Because modern browsers always show the real URL in the address bar, the threat is lessened. However, redirects can also take you to sites that will otherwise attempt to attack in other ways. For example, a redirect might take a user to a site that would attempt to trick them into downloading antivirus software and installing a Trojan of some sort instead.

Removing `referer` information

When a link is clicked, the browser sends along in the HTTP request a field called referer which indicates the source of the link. This field is populated with the URL of the current web page, and will end up in the logs of the server serving the external link. Since sensitive pages may have sensitive URLs (for example, `http://company.com/plans-for-the-next-release-of-our-product`), it is not desirable for the `referer` URL to leave the organization. A redirection page that performs referrer hiding could be embedded in all external URLs, transforming for example `http://externalsite.com/page` into `http://redirect.company.com/http://externalsite.com/page`. This technique also eliminates other potentially sensitive information from the referer URL, such as the session ID, and can reduce the chance of phishing by indicating to the end user that they passed a clear gateway to another site.

Implementation

Several different kinds of response to the browser will result in a redirection. These vary in whether they affect HTTP headers or HTML content. The techniques used typically depend on the role of the person implementing it and their access to different parts of the system. For example, a web author with no control over the headers might use a Refresh meta tag whereas a web server

The simplest technique is to ask the visitor to follow a link to the new page, usually using an HTML anchor like:

```
Please follow <a href="http://www.example.com/" >this link</a>.
```

This method is often used as a fall-back — if the browser does not support the automatic redirect, the visitor can still reach the target document by following the link.

HTTP status codes 3xx

In the HTTP protocol used by the World Wide Web, a **redirect** is a response with a status code beginning with *3* that causes a browser to display a different page. If a client encounters a redirect, it needs to make a number of decisions how to handle the redirect. Different status codes are used by clients to understand the purpose of the redirect, how to handle caching and which request method to use for the subsequent request.

HTTP/1.1 defines several status codes for redirection (RFC 7231):

- 300 multiple choices (e.g. offer different languages)
- 301 moved permanently (redirects permanently from one URL to another passing link equity to the redirected page)
- 302 found (originally "temporary redirect" in HTTP/1.0 and popularly used for CGI scripts; superseded by 303 and 307 in HTTP/1.1 but preserved for backward compatibility)
- 303 see other (forces a GET request to the new URL even if original request was POST)
- 307 temporary redirect (provides a new URL for the browser to resubmit a GET or POST request)
- 308 permanent redirect (provides a new URL for the browser to resubmit a GET or POST request)

Redirect status codes and characteristics

HTTP Status Code	HTTP Version	Temporary / Permanent	Cacheable	Request Method Subsequent Request
301	HTTP/1.0	Permanent	Yes	GET / POST may change
302	HTTP/1.0	Temporary	not by default	GET / POST may change
303	HTTP/1.1	Temporary	never	always GET
307	HTTP/1.1	Temporary	not by default	may not change
308	HTTP/1.1	Permanent	by default	may not change

[6]

All of these status codes require the URL of the redirect target to be given in the Location: header of the HTTP response. The 300 multiple choices will usually list all choices in the body of the message and show the default choice in the Location: header

(Status codes 304 not modified and 305 use proxy are not redirects).

Example HTTP response for a 301 redirect

A HTTP response with the 301 "moved permanently" redirect looks like this:

```
HTTP/1.1 301 Moved Permanently
Location: http://www.example.org/
Content-Type: text/html
Content-Length: 174
```

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.