**Hardcoded Domain in HTML**

Including a script from another domain means that the security of this web page is dependent on the security of the other domain.

**Classic Example**

<script src="http://www.example.com/js/fancyWidget.js"/>

If this tag appears on a web site other than www.example.com, then the site is dependent upon www.example.com to serve up correct and non-malicious code. If attackers can compromise www.example.com, then they can alter the contents of fancyWidget.js to subvert the security of the site. They could, for example, add code to fancyWidget.js to steal a user's confidential data.

**Example**

<script src="https://ajax.googleapis.com/ajax/libs/angularjs/1.3.9/angular-route.js"></script>

If attackers compromise the domain, they will have malicious code on this page.

**Defense Against *Specific Vulnerability***

Keep control over the code your web pages invoke. Do not include scripts or other artifacts from third-party sites.

**References**

[1] Standards Mapping - Common Weakness Enumeration, CWE ID 494, CWE ID 829

[2] Standards Mapping - NIST Special Publication 800-53 Revision 4, SC-18 Mobile Code (P2)

[3] Standards Mapping - OWASP Mobile Top 10 Risks 2014, M7 Client Side Injection

[4] Standards Mapping - SANS Top 25 2009, Risky Resource Management - CWE ID 094