Review “Browser Security”

Name: Wenhui Zhang
Email: wuz49@ist.psu.edu

Paper Name：

Anonymous(2017, Sept). Browser Security Handbook, Part 2 (Same origin policy, Life Outside Same-origin rules, Third-party cookie rules). https://code.google.com/archive/p/browsersec/wikis/Part2.wiki Sept. 2017.

Contribution:

In this paper describes 7 standard browser security features, with focusing on explicit security mechanisms and restrictions implemented, which includes: (1) same-origin policy; (2) life outside same-origin rules; (3) various network-related restrictions; (4) third-party cookie rules; (5) content handling mechanisms; (6) defenses against disruptive scripts; (7) protocol-level encryption facilities.

Motivation:

This paper does not state motivation behind implementation of browser security mechanisms. However, there exits security issues in web browsers, due to: (1) complexity of web sites and browsers; (2) large size of the Internet; (3) easy accessibility of web browser for anyone; (4) sharing of sensitive data through web browsers to reach internet. Theses factors make implementation of browser security mechanisms an urgent issue to solve.

Related works:

Web application vulnerabilities exist in various forms as discussed in this handbook, which includes (1) application mapping; (2) cookie Manipulation; (3) custom application scripting; (4) parameter manipulation; (5) reverse directory transversal; (6) cookie poisoning and theft; (7) buffer overflow through web-languages, such as javascript; (8) SQL injection; (9) cross-site scripting; (10) clickjacking etc. etc.

Methodology:

This survey style handbook reviews various vulnerabilities and their corresponding mitigation mechanisms and implementation of browser security features for field study.

Results:

Same-origin policies are defined for DOM access, XMLHttpRequest, cookies, Flash, Java, Silverlight and Gears. This paper also discussed about javascript, HTML and css vulnerabilities, and how they impact vulnerabilities while using these languages for writing websites.

Take away:

Strategies to protect oneself from being hacked while surfing websites:

1. Use NoScript extensions to prevent scripts from auto-run on websites;
2. Use pop-up blocker prevent auto-run on websites;
3. Use web of trust;
4. Disable unnecessary cookies;
5. Recognizing fake antivirus alerts;
6. Get educated on anti-phishing and anti-malware protection;
7. Block access to malicious sites and file downloads.