Deniz Aytemiz

Security Certification in Payment Card Industry: Testbeds, Measurements, and Recommendations

Currently the majority of money transactions occurring everyday are involved with PCI. Since sensitive data is being transmitted within this payment system, all entities processing sensitive information have to be compliant with the PCI Data Security Standard and be certified after certain test processes. In this paper, firstly, an e-commerce website that processes sensitive information involving manageable/changeable security vulnerabilities in architecture is built as the testbed in order to test the performances of various PCI scanners. The results are displayed in terms of all scanner's performance, which vulnerabilities they achieved to detect and rates of false positives. The results showed that the detection of vulnerabilities varies significantly across scanners yet 5 out of 6 of them were not compliant with ASV scanning guidelines and are certifying the unsecure websites. Secondly, there is the analysis of real world e-commerce websites scanning results that's developed by the authors. The results showed that 86% of the all websites scanned in the experiment had must-fix vulnerabilities meaning they are non-compliant with PCI DSS which is alarming and indicates a gap between regulations and real-life practice.[1]

Out of Sight, Out of Mind: Detecting Orphaned Web Pages at Internet-Scale

Orphaned web pages are nodes that are not linked to by any edge or any other node. This paper presents the methodology on identifying orphaned URLs of single domains. Leveraging sitemap of a website, its current and past version is compared in order to identify potential orphan pages and with heuristic least likely candidates are eliminated and rest is probed. After their methodology was experimented on large scale data, they found 1,953 possibly orphan pages on 907 unique domains. Analyzing the security measures of websites, it is resulted that orphaned pages are the least secure with being vulnerable especially to SQL injection and XSS attacks, the maintained pages on websites with orphans are more secure and fully maintained sites being most secure.[2]

Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits

Phishing is the method of impersonating authorized/trusted entities to make victims share their sensitive data. This paper presents analysis of new generation phishing toolkits and a classifier machine learning approach for detecting presence of MITM phishing toolkits using network-layer features that is 99.9% accurate. In addition, the paper mentions PHOCA, which is a fingerprinting tool that collects data and attempts to automate the detection of MITM phishing, shows many malicious website URLs are absent in blocklists. The cloaking mechanisms MITM phishing toolkits are making them more difficult to detect however by monitoring Certificate Transparency logs for domain names can successfully bypass cloaking mechanisms and makes the detection more accurate.[3]

Bibliography

[1] **[Rahaman 2019a]** Sazzadur Rahaman, Gang Wang, Danfeng Daphne Yao. Security Certification in Payment Card Industry: Testbeds, Measurements, and Recommendations. ACM CCS 2019.

[2] **[Pletinckx 2021]** Stijn Pletinckx, Kevin Borgolte, Tobias Fiebig. Out of Sight, Out of Mind: Detecting Orphaned Web Pages at Internet-Scale. ACM CCS 2021.

[3] **[Kondracki 2021]** Brian Kondracki, Babak Amin Azad, Oleksii Starov, Nick Nikiforakis: Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits. ACM CCS 2021.