



Technology
White Paper

Cenzic

Testing for Cross-Frame Scripting

Summary

For financial institutions, the risk of doing business on the Internet has recently changed somewhat dramatically as attackers increasingly target the users of such institutions directly, thus bypassing the hardened security infrastructures of these institutions. Electronic attackers and cyber criminals have strategically shifted the security playing field to one clearly in their favor - exploiting the lack of security knowledge on the part of the vast majority of users and a large footprint of potential vulnerabilities, tools, and code to leverage and exploit.

As customers, investors, and governments hold insecure companies accountable, these companies are being held liable for client side and user social engineering vulnerabilities. Being able to find and counter these threats must become a business imperative. This is especially true of financial institutions; people will not keep their money where they think it's unsafe regardless of the technical specifics. The mere appearance of lax security could easily encourage otherwise satisfied customers to switch to a competitor that appears more secure.

As if the choice of playing field hadn't already stacked the deck against the network's defenders, the lack of tools, time and expertise make it a truly daunting situation indeed. None of this information is new, nor is the security cliché that there is no absolute security, but novelty doesn't imply or confer truth or effectiveness – the only absolute in security is the need for diligence. Along these lines, Cenzic believes it can assist large institutions in their efforts increase security diligence in the area of web application security, generally, as well as, specifically, in regards to the Cross-frame Scripting Vulnerability in Internet Explorer discovered by iDefense¹.

Phishing via Cross-Frame Scripting

Phishing attacks are not new but they are increasing in frequency and sophistication. This has recently been witnessed by US, European and Asian banksⁱⁱ. So called "Phishing Scams" employ a variety of attacker techniques and Internet security failures to scam users of financial institutions into revealing their security credentials. This scam occurs usually by attackers masquerading as legitimate electronic communications from the user's financial institution.

These types of technically enabled confidence scams will continue to grow in number and sophistication as security organizations and law enforcement scramble to counter them. The simple truth is that the attackers and cyber criminals already have a huge tactical advantage because of the current insecure nature of the Internet. This tactical advantage will continue to grow as attackers' strategies evolve to counter defenders efforts; the targeting of insiders and users will only increase.

Given this situation, CenZic offers the following approach to assist financial institutions in designing, validating, and testing the safeguards and technical tools needed to verify their exposure to the Internet Explorer Cross Frame Scripting Vulnerability and its related threats.

CenZic's Approach to Solving Cross-Frame Scripting

CenZic proposes a blended approach using both software and services which combines the speed of automated testing with the thoroughness of manual penetration testing. The approach consists of two phases. The phases can be run in parallel but CenZic suggest a sequential execution through the phases to clearly baseline the code for the assessor. Phase one enables an institution to ensure the code-based safeguards of Cross Frame Scripting have been implemented. Phase two involves three steps – detection of Cross Frame Scripting Vulnerabilities, verification of the existence of a workaround, and re-test of the workaround to ensure the Cross Frame Vulnerability was implemented properly.

Phase One – Automated Checking for the Presence of Protection Mechanisms

CenZic will work with site personnel to create a custom set of detection policies through which the institution will be able to validate the presence of the appropriate code based safeguards to counter the current Cross Frame Scripting Vulnerability in Internet Explorer. These policies can be used to continuously enforce and validate such compliance, and help promote the development of more effective safeguards as Hailstorm ferrets out non-compliance.

Additionally, the process creates a known set of technical security baselines operationalized into Hailstorm policies. Such policies ideally should be developed by experienced security personnel that have an understanding of the organization's technical security infrastructure and how to use it to enforce the organization's security policies.

Once such Hailstorm policies are designed and tailored to your security infrastructure, conducting repeatable security audits no longer need be dependent on the availability of specifically skilled individuals as their testing experience has been captured in the policies they crafted. With the creation of Hailstorm Policies the experience of key staff can be leveraged and preserved.

Phase Two – Vulnerability and Safeguard Verification

Members of CenZic's CIA Research Labs have developed Cross-frame Scripting Detector solution that allows organizations to automate testing for pages that are vulnerable to display inside of frames. The solution leverages the flexibility of Hailstorm's testing approach, automated crawling and Internet Explorer to verify a page's vulnerability to Cross Frame Scripting attacks. Additionally, the results are fed back into the Hailstorm reporting engine.

With this proposed solution, CenZic will be able to craft and run a custom verification and testing policy that should be able to automate the majority of the manual testing currently necessary to verify the effectiveness of the suggested Cross Frame Scripting Vulnerability workarounds. Moreover, the solution would work to verify that the safeguard code inserted and verified in Phase One actually prevents the exploitation of the vulnerability in question or its possible variants.

Conclusion

CenZic understands that there is no "Steady State" in the security operations world and that Diligence is your only true defense. In order to meet the security testing needs of our sophisticated user base, we have crafted our approach and tools to allow flexibility, thoroughness and control. Our multi-phased approach to testing for and validating potential exposure to Cross Frame Scripting Attacks exhibits these characteristics. CenZic looks forward to assisting your organization in this matter.

Resources

ⁱ iDEFENSE Security Advisory 02.27.04b, February 27, 2004
<http://www.idefense.com/application/poi/display?id=77&type=vulnerabilities>

ⁱⁱ Hurst, Pat, 'Millions at Risk from Cyber 'Phishing' Gangs', PA News, February, 29, 2004,
<http://news.scotsman.com/latest.cfm?id=2589922>

Colley, Andrew, "Most devious" bank email phishing scam discovered: Fraudsters getting cleverer and cleverer", Silicon.com, March 04 2004

<http://www.silicon.com/software/security/0,39024655,39118902,00.htm>