



Testing for Cross-Frame Scripting

Overview of Web Application Vulnerabilities
Exploited by Hackers



Table of Contents

Executive Summary	3
Phishing via Cross-Frame Scripting	3
Cenzic’s Approach to Solving Cross-Frame Scripting.....	3
Phase One – Automated Checking for the Presence of Protection Mechanisms.....	4
Phase Two – Vulnerability and Safeguard Verification	4
Conclusion	4
Resources	4
About Cenzic	5



Executive 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 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.

The lack of tools, time and expertise makes security 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, 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 banks². 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 and 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 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 Cenzic ferrets out non-compliance.

Additionally, the process creates a known set of technical security baselines operationalized into Cenzic's policies. Such policies 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 Cenzic's policies are designed and tailored to your security infrastructure, conducting repeatable security audits no longer needs 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 Cenzic's 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 development a 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 Cenzic'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 Cenzic's reporting engine.

With this solution, Cenzic will be able to craft and run a custom verification and testing policy that automates the majority of the manual testing currently necessary to verify the effectiveness the suggested Cross Frame Scripting Vulnerability workarounds. Moreover, the solution works 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.

Resources

¹DEFENSE Security Advisory. 02.27.04b, February 27, 2004.

<http://www.idefense.com/application/poi/display?id=77&type=vulnerabilities>

²Hurst, 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 4, 2004.

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



About Cenzic

Cenzic provides an application security intelligence platform to continuously assess Cloud, Mobile and Web vulnerabilities. This helps brands of all sizes protect their reputation and manage security risk in the face of malicious attacks. Today, Cenzic secures more than half a million online applications and trillions of dollars of commerce for Fortune 1000 companies, all major security companies, government agencies, universities and SMBs.

Cenzic Products

Cenzic Enterprise	Cenzic Enterprise is a software solution that assesses the security of Cloud and Web applications and supports security risk management throughout the software development lifecycle. Cenzic Enterprise provides a company-wide view of security vulnerabilities and status to executives as well as customized views for other users from a Web-based dashboard.
Cenzic Desktop	Cenzic Desktop is a single-user version of Cenzic Enterprise. It is designed for the power user that wants to run their security assessments on Cloud and Web applications from a single system.
Cenzic Managed Cloud	With Cenzic Managed Cloud, Cenzic's security experts remotely perform full vulnerability testing on Cloud, Mobile and Web applications. From a Web-based dashboard, users can request assessments, view results, run reports, analyze trends and re-test applications to verify remediation efforts.
Cenzic Cloud	Cenzic Cloud allows users to test their own Cloud and Web applications for basic attacks and receive actionable results all within their own Web portal – no security experts needed.
Cenzic Hybrid – Software + Cloud	Cenzic Hybrid provides access to both Cenzic Enterprise software and Cenzic Managed Cloud services. Vulnerability testing can be done either by using the software on premise or by leveraging Cenzic's expert security services team.
Cenzic Mobile	Cenzic Mobile service is delivered as a managed service. Cenzic's security experts remotely perform full vulnerability testing on mobile applications. All testing is managed from a Web-based dashboard where users can request assessments, view results, run reports, analyze trends and re-test applications to verify remediation efforts.
Cenzic Services	Cenzic services and training help those responsible for Cloud, Mobile and Web application security to implement best practices and procedures to protect data from hacker attacks.