Top Claim- Magento minimizes malicious code

It would be a challenging task for Magento to completely avoid the injection of malicious code into the system. Magento tries its best to reduce the risk of malicious code being introduced into

the code. By following few of the best practices it tries to be resilient to risks introduced by malicious code injection. In our claim we begin our discussion with a rebuttal R1 that unless

Magento is injected with malicious code, the software is secure. Our Sub Claim C3.1 assures that Magento follows all the security policies and guidelines, that reduces the risk of Magento

being injected with malicious code.

**Evidence E3.1**

Our Sub Claim C3.1 leads to rebuttal R2, what if the software is not up to date. We address this question with Sub Claim C3.2 where Magento ensures to notify its users with updates

on the latest patches. The Evidence E3.1 for this claim is the Magento Security Center, where it gathers all the information about the latest patches, security updates, notifications and best

security practices to be followed .<https://magento.com/security> Magento publishes all the hotfixes on the Magento Security Center that contain high-impact security or quality fixes that affect many Magento merchants. It has introduced a Security Alert Registry which is a mailing list that receives updates every time there is a potential security vulnerability or Magento patch. Thus, ensuring all

its users are informed about the latest security patches.

Evidence E3.2

We also have our Sub Claim C3.3 which addresses rebuttal R2, which states that Magento provides a scanner for identifying missing or infected patches. Evidence E3.2 provides the evidence for this

subclaim through a mage report. Magneto provides an option to scan our site on magereport.com to identify any missing security patches and to determine if it has been infected with known malware strains.

<https://magento.com/security/best-practices/remediating-your-site-after-malware-attack>

Evidence E3.3

Our Sub Claim C3.1 also leads to rebuttal R3, which argues that what if unnoticed malicious code has been introduced into the software. Sub Claim C3.4 addresses this rebuttal by stating that Magento performs scanning to detect if some malicious code has been introduced. Evidence E3.3 shows the evidence for this subclaim, where Magento provides its users a Security scan tool

that enables Magento merchants to regularly monitor their sites and receive updates regarding known security risks, malware, and unauthorized access. Security Scan is a free service of

Magento and can be run on any version of Magento Commerce and Magento Open Source. <https://magento.com/blog/magento-news/introducing-new-magento-security-scan-tool>

It scans result reports that show which checks the site has passed and failed and whether further action is required, provides details on the schedules of specific scans, and suggests

remediation steps for each failed security test.

Evidence E3.4

UM1 undermines our evidence E3.3 questioning the frequency of the scans performed by Magento and what would happen if the scans are not performed regularly. Our Sub Claim C3.5 answers this question, stating that Magento provides regular security checks and also notifies its users about the same. The evidence for this is provided in the Magento security documentation .https://www.adobe.com/content/dam/acom/en/security/pdfs/Adobe-Magento-Commerce-BestPractices-Guide.pdf

The documentation clearly states that the Magento security scan service, allows us to monitor our magneto sites for known security risks and security notifications.

It provides an option to schedule security scans to run weekly, daily or on demand. It also maintains a history of security reports in the individual accounts.

Evidence E3.5

Our Sub Claim C3.1 also leads to rebuttal R4, which argues about the consequences of Magento being attacked by Cross Site Scripting (XSS) attack. But Sub Claim C3.6 assures that rebuttal by

stating that Magento provides an option to configure CSP (Content Security Policies) headers. The CSP are a powerful tool to mitigate XSS attacks and the other related attacks like card skimming,

session hijacking, clickjacking, and other malware related attacks. Evidence E3.5 provides evidence for this claim through a CSP report where Magento reports the policy violations which

is useful for debugging. <https://devdocs.magento.com/guides/v2.4/extension-dev-guide/security/content-security-policies.html>

CSP's built-in browser prevents loading malicious script from an attacker's website and also from sending the credit card info to the attacker's website.

Evidence E3.6

UM2 undermines our evidence E3.5 questioning the possibility of users needing some assistance to fix the violation identified by the CSP report. Thus the Sub Claim C3.7 assures that Magento

provides the restrict mode option where it can help the users to resolve the violation. The evidence for this subclaim is provided in E3.6 in respect to Magento's restrict mode. In this mode, Magento acts on any policy violations.

Policies can be configured for admin html and storefront areas separately to accommodate different use cases. Magento also permits configuring unique CSPs for specific pages.

<https://devdocs.magento.com/guides/v2.4/extension-dev-guide/security/content-security-policies.html>

Evidence E3.7

We also have our Sub Claim C3.8 which addresses rebuttal R4, which argues that Magento provides OWASP ruleset for filtering cross site injection attacks which can minimize the risk of XSS attack.

Evidence E3.7 provides the evidence for that subclaim with help of Magento WAF report. The OWASP ruleset protects against cross-site injection attacks.

It leverages a mechanism for each request looking for cross-site injection and other threats to the origin and scores every request against the entire core ruleset

and validates that the request score.

<https://support.magento.com/hc/en-us/articles/360016353452--Web-Application-Firewall-WAF-powered-by-Fastly-the-FAQ>