Document Purpose

This document provides important information for Engaging Networks' clients when evaluating and configuring alternate (non-Control Case) PCI-DSS Approved Scanning Vendor (ASV) scanners. It highlights critical considerations, particularly regarding the accurate scanning of directory structures, which many ASV scanners fail to perform correctly using default settings. Without this guidance, ASV scans may be incomplete or inadvertently include additional web pages that are not part of the PCI DSS cardholder data environment. The information outlined here is intended to ensure proper configuration and optimization of ASV scan settings for compliance and practical security assessments.

Donation Page Structure

Engaging Networks is a PCI-DSS Level 1 service provider that hosts multiple client payment pages using its custom host domain (DNS). The page's root (for example, donate.domain1.org) is not part of the Cardholder Data Environment (CDE); all pages comprised of the CDE are subdirectories. Below are examples of 2 different client site directory structures.

The /page/* subdirectories are hosted within our environment and are part of the CDE. However, we do not host the root domain or any other pages, nor are they part of the CDE.

Each endpoint (donation page) could use different JavaScript libraries (that are not hosted, reviewed, or vetted by Engaging Networks). Depending on the page's development, individual pages could have XSS or DCOM vulnerabilities.

Host domain (not part of the CDE, do not scan)	Subdirectories (part of CDE, need to scan and group under the host domain)
donate.domain1.org	/page/24642/1/ /page/26647/1/ /page/26956/1/ /page/37808/1/ /page/37809/1/ /page/38070/1/ /page/38110/1/ /page/38124/1/ /page/38129/1/ /page/38139/1/ /page/38140/1/ /page/3924/1/ /page/47327/1/ /page/47514/1/ /page/47515/1/ /page/47688/1/

	/page/47810/1/ /page/48438/1/ /page/59582/1/ /page/59583/1/ /page/71982/1/ /page/71983/1/ /page/72988/1/ /page/77222/1/ /page/82404/1/ /page/82405/1/ /page/82723/1/ /page/82724/1/ /page/82805/1/ /page/85185/1/ /page/86305/1/ /page/86306/1/
donate.domain2.org	/page/105680/1/ /page/105981/1/ /page/106896/1/ /page/110281/1/ /page/111079/1/ /page/111343/1/ /page/111345/1/ /page/112386/1/ /page/112955/1/ /page/121196/1/ /page/129045/1/ /page/132726/1/ /page/132730/1/ /page/132844/1/ /page/134112/1/ /page/144839/1/

Additional Information

Engaging Networks clients often configure custom donation hostnames, such as donate.domain1.org or donate.domain2.org, to redirect traffic from the root domain (https://donate.domain1.org) to pages outside the PCI-DSS Cardholder Data Environment (CDE). These redirections typically lead to external destinations, such as a client's landing page or an Engaging Networks corporate page, which are not within the scope of PCI-DSS compliance because they do not process, store, or transmit cardholder data.

For instance, traffic to https://donate.domain1.org may be redirected to https://www.clientdomain.com/landing-page or https://engagingnetworks.net. These external pages exist outside the CDE, avoiding inclusion in compliance audits. However, redirects at the top

level of the custom domain can inadvertently cause Approved Scanning Vendor (ASV) tools to scan content that is not part of the intended PCI-DSS scope. This can lead to unnecessary or false findings, complicating compliance validation and potentially increasing the risk of audit failures.

To prevent these issues, it is strongly recommended that redirects from the top level of the custom domain (https://donate.domain1.org) be disabled. This ensures that ASV scanners are not inadvertently redirected to non-CDE content, reducing the likelihood of scanning errors or scope misconfigurations. Without a redirect, traffic to the top-level domain will not lead to external destinations, causing unintended scanning.

In cases where disabling top-level redirects is not feasible, organizations must ensure that ASV scanner configurations are explicitly set to exclude the top-level domain and any non-CDE redirection targets. Scanners should focus solely on the specific donation pages within the CDE, such as https://donate.domain1.org/page/24642/, which handle sensitive payment information.

If you use page redirects, it is essential that you know how these are used. Similarly to the root domain redirect, page redirects could inadvertently cause the ASV scanner to scan beyond the CDE. It is the customer's responsibility to ensure that this does not occur.

More information on Engaging Networks redirects can be found here:
https://knowledge.engagingnetworks.net/pagebuilder/advanced-redirect-page-redirect

Properly managing redirects and configuring scanning tools are critical steps to streamlining PCI-DSS compliance. By preventing ASV scanners from following unnecessary redirects and limiting the scope of scans to relevant CDE environments, clients can reduce false positives, simplify the compliance process, and maintain a clear separation between PCI-DSS and non-CDE systems.