Nmap Scan Result

a. Summary - No. of Vulnerable Ports Open

Total Count : : **2**

b. Detailed Report

i. Port Number: 80

ii. Protocol: tcp

iii. Service: http

iv. Recommended Action or Best Practices: Apply security headers, keep software updated, and implement secure coding practices.

i. Port Number: 443

ii. Protocol: tcp

iii. Service: https

iv. Recommended Action or Best Practices: Apply security best practices for HTTPS services.

ZAP Scan Result

a. Summary

i. No. of Total Vulnerabilities Identified: : 29

ii. No. of Total Vulnerabilities Identified grouped on Risk Rating: : {'Informational': 11, 'Low': 13, 'Medium': 5}

b. Detailed Report

i. Vulnerability Summary: Retrieved from Cache

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

v. Details to Reproduce the Instance:

- **URL:** http://quarksek.com/_api/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Age: 0

i. Vulnerability Summary: Retrieved from Cache

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

v. Details to Reproduce the Instance:

- **URL:** http://quarksek.com/robots.txt
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Age: 0

i. Vulnerability Summary: Retrieved from Cache

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

v. Details to Reproduce the Instance:

- **URL:** http://quarksek.com/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Age: 3

i. Vulnerability Summary: Retrieved from Cache

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

v. Details to Reproduce the Instance:

- **URL:** http://quarksek.com
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Age: 3

i. Vulnerability Summary: Retrieved from Cache

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

v. Details to Reproduce the Instance:

- **URL:** http://quarksek.com/sitemap.xml
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Age: 0

i. Vulnerability Summary: Retrieved from Cache

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

v. Details to Reproduce the Instance:

- **URL:** http://quarksek.com/*?lightbox
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Age: 0

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** http://quarksek.com
- **Method:** GET
- **Parameter:** X-Wix-Request-Id
- **Attack:** No attack specified
- **Evidence:** 1710755668

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** http://quarksek.com/robots.txt
- **Method:** GET
- **Parameter:** X-Wix-Request-Id
- **Attack:** No attack specified
- **Evidence:** 1710755669

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** http://quarksek.com/
- **Method:** GET
- **Parameter:** X-Wix-Request-Id
- **Attack:** No attack specified
- **Evidence:** 1710755669

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** http://quarksek.com/_api/
- **Method:** GET
- **Parameter:** x-wix-request-id
- **Attack:** No attack specified
- **Evidence:** 1710755669

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** http://quarksek.com/*?lightbox
- **Method:** GET
- **Parameter:** x-wix-request-id
- **Attack:** No attack specified
- **Evidence:** 1710755669

i. Vulnerability Summary: Retrieved from Cache

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

v. Details to Reproduce the Instance:

- **URL:** http://quarksek.com/pro-gallery-webapp/v1/galleries/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Age: 0

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** http://quarksek.com/sitemap.xml
- **Method:** GET
- **Parameter:** x-wix-request-id
- **Attack:** No attack specified
- **Evidence:** 1710755668

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** http://quarksek.com/_partials
- **Method:** GET
- **Parameter:** X-Wix-Request-Id
- **Attack:** No attack specified
- **Evidence:** 1710755669

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** http://quarksek.com/pro-gallery-webapp/v1/galleries/
- **Method:** GET
- **Parameter:** X-Wix-Request-Id
- **Attack:** No attack specified
- **Evidence:** 1710755669

i. Vulnerability Summary: Cross-Domain Misconfiguration

ii. Risk Rating: Medium

iii. Confidence Rating: Medium

iv. Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server

v. Details to Reproduce the Instance:

- **URL:** http://quarksek.com/_partials/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Access-Control-Allow-Origin: *

i. Vulnerability Summary: Retrieved from Cache

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

v. Details to Reproduce the Instance:

- **URL:** http://quarksek.com/_partials/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Age: 0

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** http://quarksek.com/_partials/
- **Method:** GET
- **Parameter:** X-Wix-Request-Id
- **Attack:** No attack specified
- **Evidence:** 1710755670

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** http://example.com/sitemap.xml
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Missing Anti-clickjacking Header

ii. Risk Rating: Medium

iii. Confidence Rating: Medium

iv. Description: The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.

v. Details to Reproduce the Instance:

- **URL:** http://example.com
- **Method:** GET
- **Parameter:** x-frame-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** http://example.com/robots.txt
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Retrieved from Cache

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

v. Details to Reproduce the Instance:

- **URL:** http://example.com/sitemap.xml
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Age: 390183

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** http://example.com
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Retrieved from Cache

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

v. Details to Reproduce the Instance:

- **URL:** http://example.com/robots.txt
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Age: 391809

i. Vulnerability Summary: Server Leaks Version Information via "Server" HTTP Response Header Field

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

v. Details to Reproduce the Instance:

- **URL:** http://example.com/sitemap.xml
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** ECS (nyd/D164)

i. Vulnerability Summary: Server Leaks Version Information via "Server" HTTP Response Header Field

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

v. Details to Reproduce the Instance:

- **URL:** http://example.com/robots.txt
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** ECS (laa/7B4B)

i. Vulnerability Summary: Retrieved from Cache

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

v. Details to Reproduce the Instance:

- **URL:** http://example.com
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** HIT

i. Vulnerability Summary: Server Leaks Version Information via "Server" HTTP Response Header Field

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

v. Details to Reproduce the Instance:

- **URL:** http://example.com
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** ECS (laa/7BA4)

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** http://example.com
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified

- **Evidence:** No evidence available