Website performance and security analysis

Issues

Security

Issues addressed

- Website response header is exposed (shows that server is running IIS, PHP and their version).

- Response header doesn't follow common best practices for security. (ref: https://owasp.org/www-project-secure-headers/)

- Website doesn't block phpMyAdmin and wp-admin from outside IP

- Permissions for the web folder should only be limited to only what is needed to run the website.

- Few image sources link have not been updated to the latest domain yet and still uses HTTP.

- Parts of the website allow cross-origin resource sharing to any host.
  Categorized as Firm (confirmed).
  Please refer Burp Suite report attached.

- SQL Injection vuln may be present but Burp Suite only reports it once.
  Categorized as tentative (not certain, no confidence)
  Please refer Burp Suite report attached.

- There are two high risks security issues detected by Burp Suite:
  1. Cross-Origin Resource Sharing (9) (Firm) (confirmed).
  2. SQL Injection (1) (Tentative) (not certain, no confidence).

  (number of reports)(category)(category meaning)

Performance

Issues addressed

- Website is too slow to load. (image size is too big)
- Website might not handle high load well in the future due to hardware limitations (CPU RAM).

Action

Security

Action taken

- Removed IIS server header using Powershell and removed PHP headers by editing php.ini

  Powershell

  ```
  Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST/deftech'  -filter "system.webServer/security/requestFiltering" -name "removeServerHeader" -value "True"
  Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST'  -filter "system.webServer/security/requestFiltering" -name "removeServerHeader" -value "True"
  ```

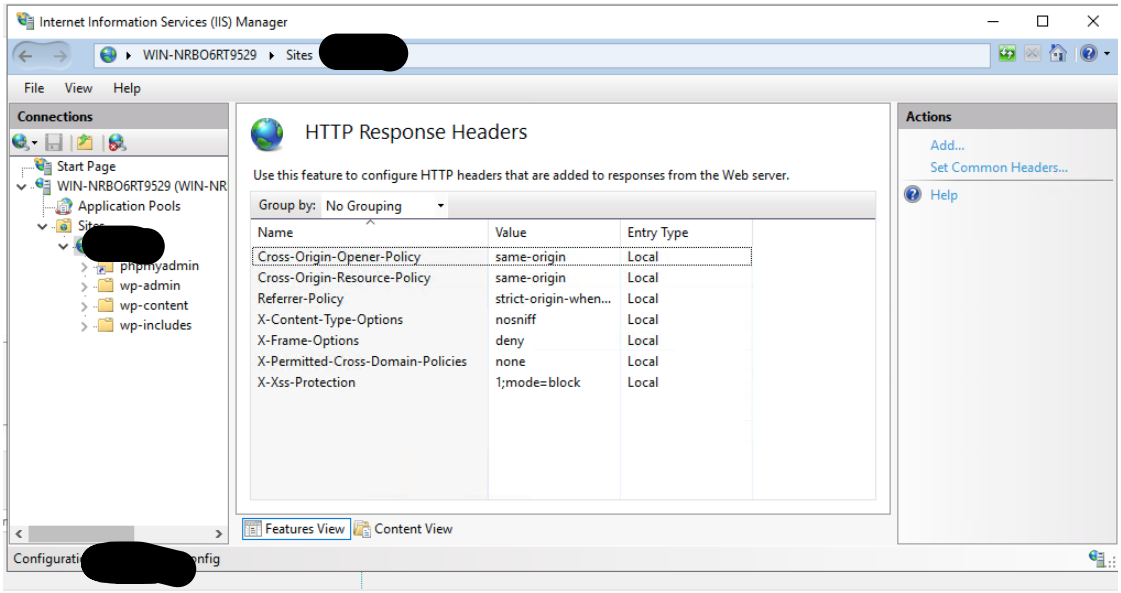
  PHP.ini

  ```
  expose_php=Off
  ```

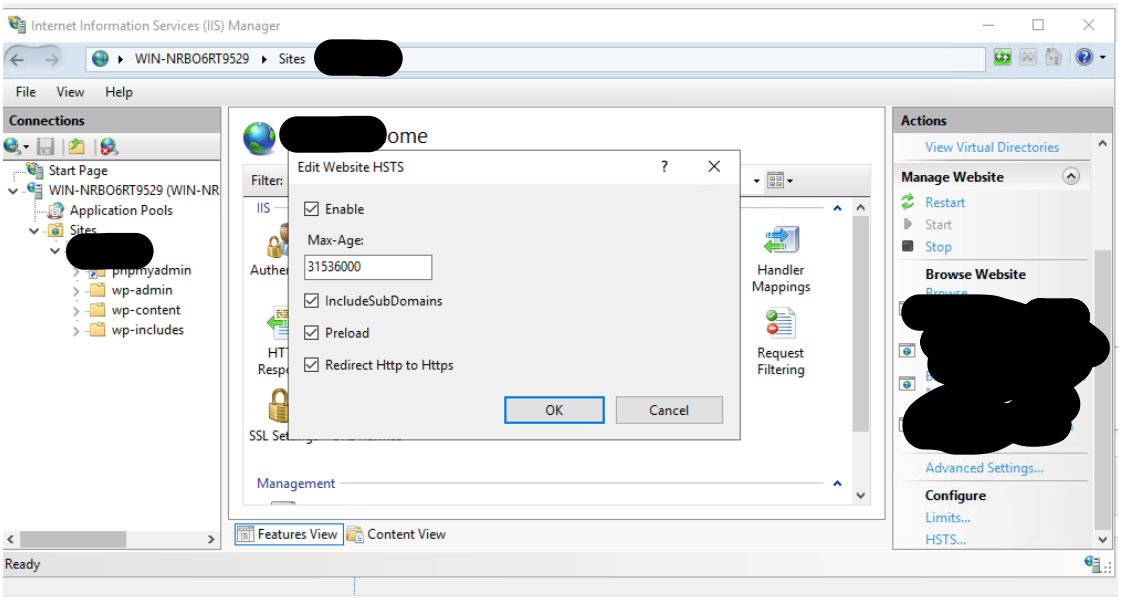
  Issues encountered :

  None. Headers removed successfully.

- Added few response headers that is considered as best practice according to OWASP. Also added HSTS (HTTPS Strict Transport Security) (ref: https://owasp.org/www-project-secure-headers/)



Adding custom headers



Enabling HSTS (HTTP Strict Transport Security)

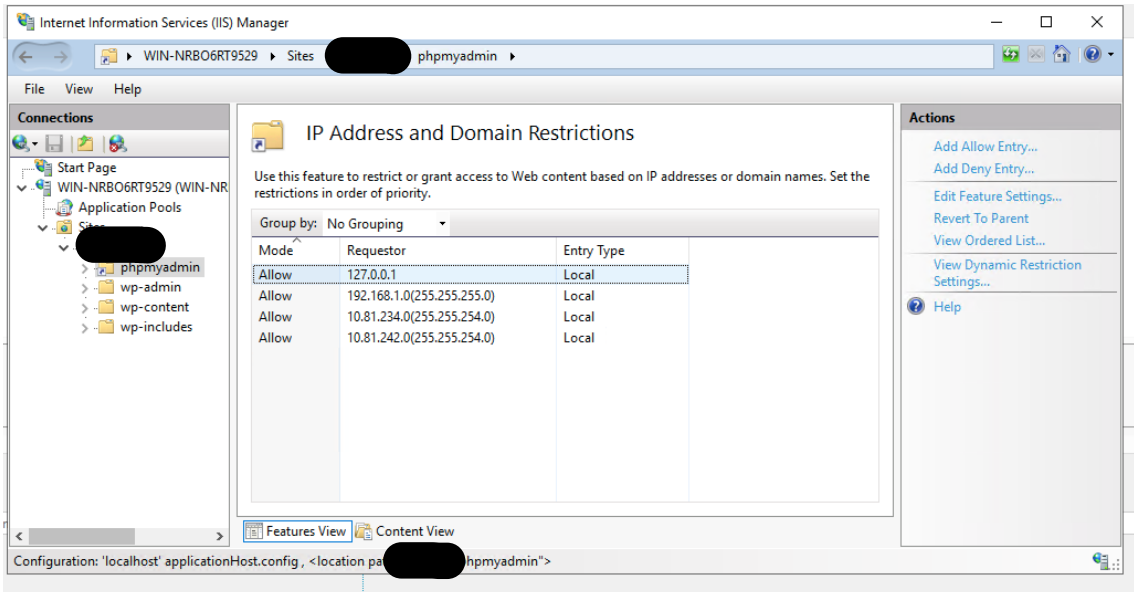
Issues encountered :

One of the headers that is recommended by OWASP can’t be used because it was too restrictive
(Specific header name: Content-Security-Policy)

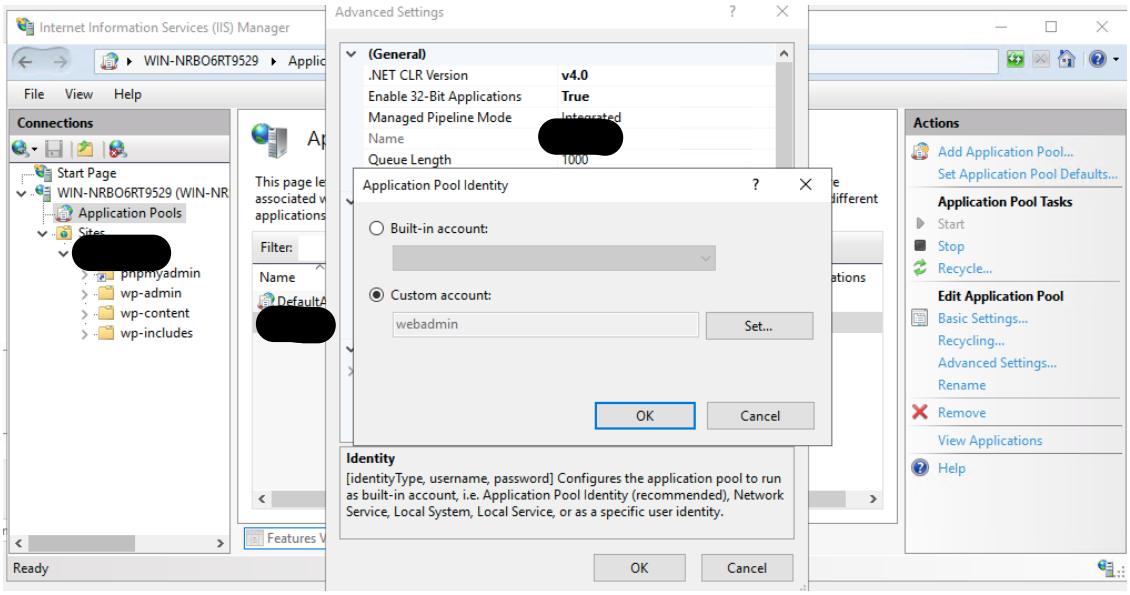
Content-Security-Policy limits the location of the resources the browser can access. This will break the website if not configured properly.

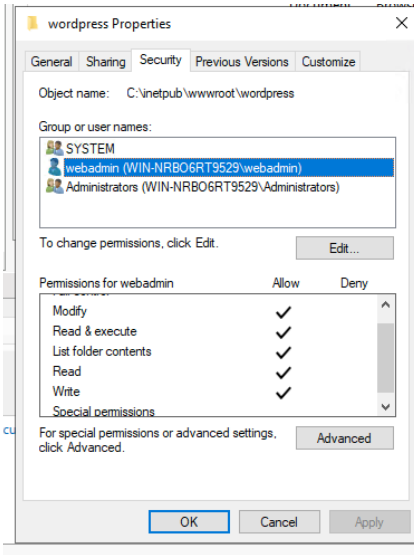
Content-Security-Policy should be added once the website is finalized. Only then we can define locations that should be trusted to be accessed.

- Blocked access from outside to phpMyadmin and wp-admin folder. (folder is set to deny on any connections except the IP stated below)



- Added a new user (webadmin) to run the website. Limit the permissions to only what is needed.





Issues encountered:

None.

- Installed Really Simple SSL plugin for Wordpress to force all links inside website to change from HTTP to HTTPS

  (ref: https://wordpress.org/plugins/really-simple-ssl/)

  Issues encountered:
  None

- Installed Prevent XSS Vulnerability Wordpress plugin to block symbols that can be input into the system for XSS attacks.

  (ref: https://wordpress.org/plugins/prevent-xss-vulnerability/)

  Issues encountered :

  Can't bulk delete posts.

- Removed unused Wordpress Posts as some of them may pose a security risk. (This is where SQL Injection is reported once but it's categorized as tentative) (tentative = unsure, not certain)

  Issues encountered:
  None

- Add header Access-Control-Allow-Origin only for [redacted]
  (This is for Cross-Origin Resource Sharing arbitrary origin trusted issue reported by Burp Suite)

  Access-Control-Allow-Origin: [redacted]

  This header setting will make sure only [redacted] will be able to fetch data from this website.

  Issues encountered:
  None

- Uninstall unused themes,updated the current theme and plugins.

  Issues encountered:
  None

Performance

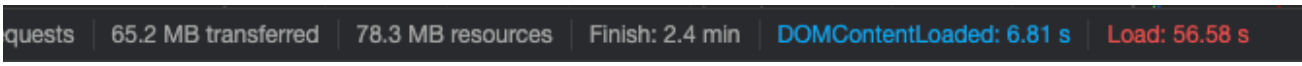
Action taken

- Installed PHP extension Zend Opcache and APCU for caching website. Caching using these extension will make the website faster but it uses a lot of server resources so it is recommended to have a decent amount of RAM for caching.

  Issues encountered:

  Images file size is too big. Images need to be compressed or have reduced resolution for the website to load faster.

  (78.3mb to load the front page)



Suggested actions

(*) = Strongly suggested

- **(*)** Compress or reduce image resolution to make the website load faster.
- **(*)** Increase server CPU and RAM capacity for better caching and request performance
- **(*)** Configure Content-Security-Policy headers once the website is finalized.
- **(*)** Rescan with Burp Suite once everything has been finalized.
- Update Wordpress plugins and themes
- Remove unused plugins