NIKTO- METASPLOITABLE 3

192.168.1.19/PHPMYADMIN

VULNERABILIDADES.

- https://developer.mozilla.org/es/docs/Web/HTTP/Headers/X-Frame-Options

El encabezado de respuesta HTTP X-Frame-Options puede ser usado para indicar si debería permitírsele a un navegador renderizar una página en un <frame>, <iframe>, <embed> u <object>. Las páginas web pueden usarlo para evitar ataques de click-jacking, asegurándose de que su contenido no es embebido en otros sitios.

Existen dos posibles directivas para X-Frame-Options:

X-Frame-Options: DENY - La página no puede ser mostrada en un marco, independiente del sitio que esté intentándolo.

X-Frame-Options: SAMEORIGIN - La página sólo puede ser mostrada en un marco del mismo origen que dicha página.

Clickjacking es la práctica de engañar a un usuario en hacer clic en un enlace, botón, etc. que no es lo que el usuario cree que es. Esto puede ser usado, por ejemplo, para robar credenciales de inicio de sesión o para obtener el permiso indeseado para instalar una pieza de malware. (Clickjacking se llama a veces "redes de la interfaz de usuario", aunque este es un uso equivocado del término "redress").

- X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.

Explicación:

Falta un Content-Typeheader, lo que significa que este sitio web podría estar en riesgo de sufrir ataques de rastreo MIME.

El rastreo de tipos MIME es una funcionalidad estándar en los navegadores para encontrar una forma adecuada de representar datos donde los encabezados HTTP enviados por el servidor no son concluyentes o faltan.

Esto permite que las versiones anteriores de Internet Explorer y Chrome realicen un rastreo MIME en el cuerpo de la respuesta, lo que potencialmente hace que el cuerpo de la respuesta se interprete y se muestre como un tipo de contenido distinto al tipo de contenido previsto.

El problema surge cuando un sitio web permite a los usuarios cargar contenido que luego se publica en el servidor web. Si un atacante puede llevar a cabo un ataque XSS (Cross-site Scripting) manipulando el contenido de manera que sea aceptado por la aplicación web y representado como HTML por el navegador, es posible inyectar código, por ejemplo, en un archivo de imagen y hacer que la víctima lo ejecuta viendo la imagen.

- Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.

https://www.cve.org/CVERecord?id=CVE-2017-9798

Descripción:

Apache httpd permite a atacantes remotos leer datos secretos de la memoria del proceso si se puede establecer la directiva Limit en el archivo .htaccess de un usuario, o si httpd.conf tiene ciertas configuraciones erróneas, también conocido como Optionsbleed. Esto afecta al Servidor HTTP Apache hasta 2.2.34 y 2.4.x hasta 2.4.27. El atacante envía una petición HTTP OPTIONS no autenticada al intentar leer datos secretos. Se trata de un problema de "use-after-free", por lo que los datos secretos no siempre se envían, y los datos específicos dependen de muchos factores, incluida la configuración. La explotación con .htaccess puede bloquearse con un parche a la función ap_limit_section en server/core.c.

El servidor web devuelve una respuesta válida con métodos HTTP no deseados que puedan causar falsos positivos. - Por lo general, esto significa que el sitio está utilizando algún tipo de funcionalidad de ruta de URL, es decir, ng-route o $.route/$. Nota.

- OSVDB-12184:

Muchos webadmins cuando tratan con PHP y seguridad usan varios trucos como la falsificación de banners, etc. Pero muchos no saben de una broma oculta dentro de PHP: un Easteregg dejado por los desarrolladores. Puede ser revelado enviando una consulta GET especialmente diseñada.