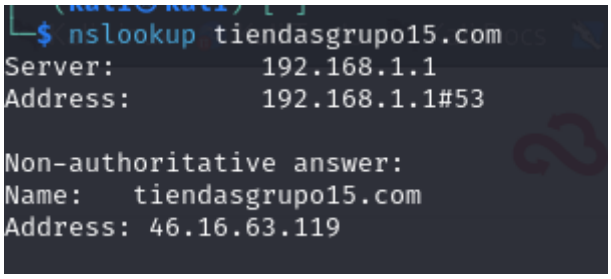
NIKTO – GRUPO15

http://tiendasgrupo15.com

Hacemos un nslookup a la pagina web de la víctima.

Nos da la dirección ip: **46.16.63.119**



Seguidamente hacemos el comando nikto -url www.tiendasgrupo15.com

Dándonos los resultados más abajo:

Indagando un poco más en los datos obtenidos mediante nikto vemos lo siguiente:

- Target IP:46.16.63.119
- Target Hostname: 46.16.63.119
- Target Port: 80
- Start Time: 2023-11-22 06:22:33 (GMT-5). Podemos deducir que el servidor se encuentra en el huso horario GMT-5 (probablemente Nueva York, México,etc…)
- Server: Apache
- /80/: The anti-clickjacking X-Frame-Options header is not present:

  El encabezado de respuesta HTTP X-Frame-Options se puede utilizar para indicar si se debe permitir o no a un navegador mostrar una página en un <frame>, <iframe>, <embed> o <object>. Los sitios pueden utilizarlo para evitar ataques de click-jacking, asegurándose de que su contenido no está incrustado en otros sitios.

  Clickjacking es la práctica de engañar a un usuario para que haga clic en un enlace, botón, etc. que es distinto de lo que el usuario cree que es.

- /80/: The 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.

Falta la cabecera Content-Type, lo que significa que este sitio web podría estar expuesto a un ataque MIME-sniffing.

El rastreo de tipos MIME es una funcionalidad estándar de los navegadores para encontrar una forma adecuada de presentar los datos cuando las cabeceras HTTP enviadas por el servidor no son concluyentes o faltan.

Esto permite a las versiones más antiguas de Internet Explorer y Chrome realizar el rastreo de MIME en el cuerpo de la respuesta, lo que puede provocar que el cuerpo de la respuesta se interprete y se muestre como un tipo de contenido distinto al previsto.

- OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD.

Podemos usar los distintos métodos citados arriba para obtener más información.