Ciudad de México, a 12 de julio de 2021

JOSE LUIS GONZALEZ HERNANDEZ
COORDINADOR DE DESARROLLOS
DE SISTEMAS INSTITUCIONALES

PRESENTE

Por este medio me permito enviar a usted de forma impresa los resultados obtenidos referente a la url:

https://aplicaciones.finanzas.cdmx.gob.mx/educad/public/inicio

Sin otro particular, aprovecho la ocasión para enviarle un cordial saludo.

ATENTAMENTE

ULISES ANDRES CARRANZA MARTÍNEZ
JUD DE SEGURIDAD INFORMÁTICA

UACM

Vulnerabilidades

Sistema	Vulnerabilidad alta	Vulnerabilidad media	Vulnerabilidad baja
https://aplicaciones.finanzas.cdmx.gob.mx/educad/public/inicio	0	10	2

INFORMACIÓN OBJETIVO

SERVIDOR	APACHE/2.4.25 (Debian)
SISTEMA OPERATIVO	Unix
TECNOLOGIAS IDENTIFICADAS	
SENSIBLE	Si

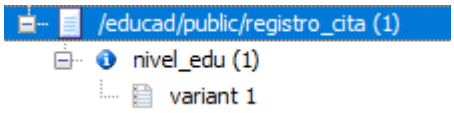
Vulnerabilidades Medias

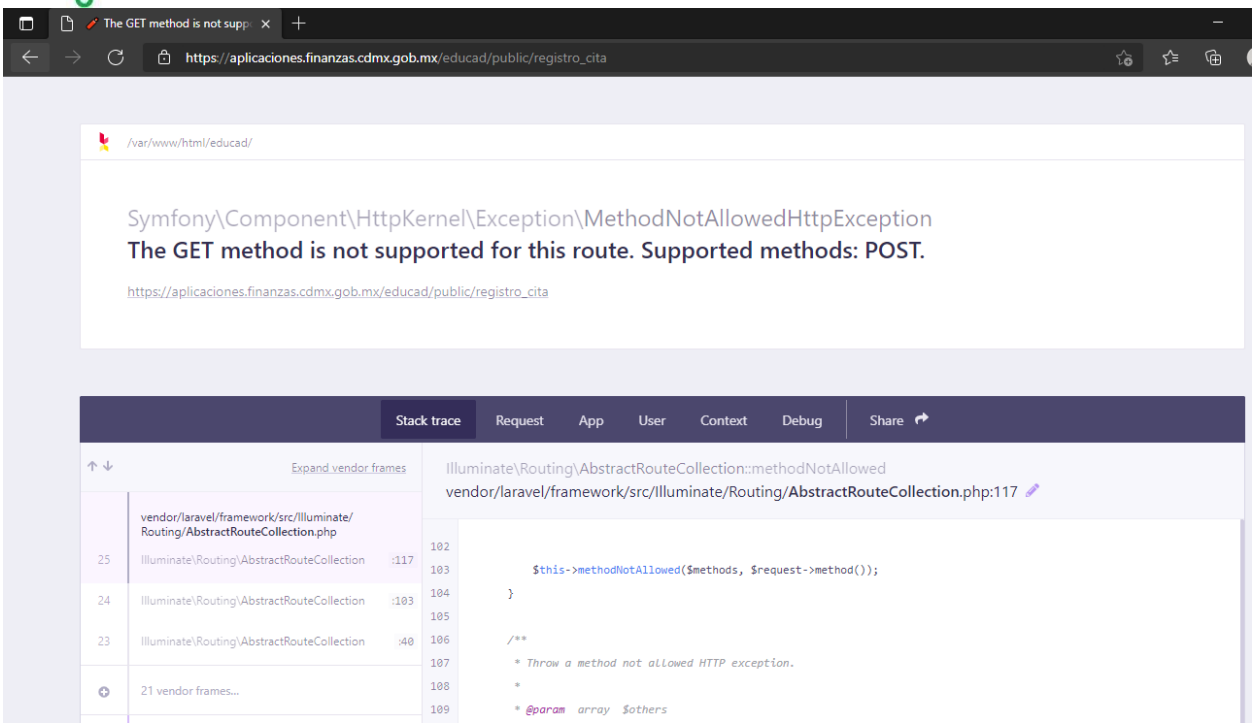
Application error message

Esta página contiene un mensaje de error/advertencia que puede revelar información confidencial. El mensaje también puede contener la ubicación del archivo que produjo la excepción no controlada.

Esto puede ser un falso positivo si el mensaje de error se encuentra en las páginas de documentación.

Afecta a:





El impacto de esta vulnerabilidad

Los mensajes de error pueden revelar información confidencial. Esta información se puede utilizar para lanzar nuevos ataques

Remediación:

Omita estas rutas para no exponer posible información.

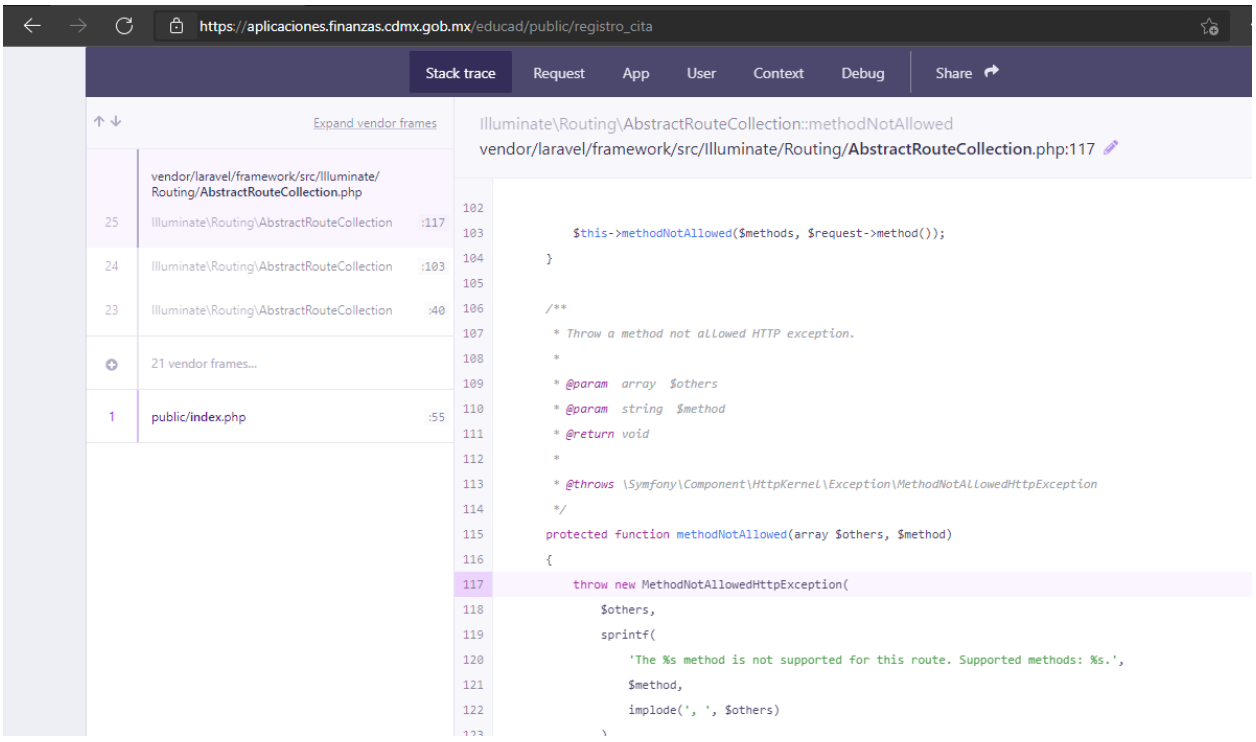
Internal server error(8)

Descripción de la vulnerabilidad

Esta página contiene un mensaje de error / advertencia que puede revelar información confidencial. El mensaje también puede contener la ubicación del archivo que produjo la excepción no controlada.

Afecta a:

- /educad/public/ (2)
  - laravel_session (1)
    - variant 1
  - XSRF-TOKEN (1)
    - variant 1
- /educad/public/inicio (2)
  - laravel_session (1)
    - variant 1
  - XSRF-TOKEN (1)
    - variant 1
- /educad/public/registro_cita (2)
  - nivel_edu (1)
    - variant 1
  - rfc (1)
    - variant 1
- /educad/public/seguridad/login (2)
  - laravel_session (1)
    - variant 1
  - XSRF-TOKEN (1)
    - variant 1



Cómo solucionar esta vulnerabilidad

Revise el código fuente de este script y omita el acceso a ese tipo de directorios.

Slow HTTP Denial of Service Attack

Su servidor web es vulnerable a ataques de denegación de servicio HTTP lentos.

Los ataques Slowloris y Slow HTTP POST DoS se basan en el hecho de que el protocolo HTTP, por diseño, requiere que el servidor reciba las solicitudes por completo antes de procesarlas. Si una solicitud HTTP no está completa o si la tasa de transferencia es muy baja, el servidor mantiene ocupados sus recursos esperando el resto de los datos. Si el servidor mantiene ocupados demasiados recursos, esto crea una denegación de servicio.

Afecta a:

Web Server

El impacto de esta vulnerabilidad

Una sola máquina puede desactivar el servidor web de otra máquina con un ancho de banda mínimo y efectos secundarios en servicios y puertos no relacionados.

Remediación

Medidas de protección en la red interna

Cuando la página web se encuentra en la red interna de la empresa se han de incorporar elementos de protección perimetral para protegerlo. Entre otras medidas:

Ubicar el servidor web en una zona desmilitarizada (entre cortafuegos), también llamada DMZ, evitando así que un intruso pueda acceder a la red interna si vulnera el servidor web; implementar un sistema de detección y prevención de intrusiones (IDS/IPS) que monitorizan las conexiones y nos alerta si detecta intentos de acceso no autorizados o mal uso de protocolos; utilizar un dispositivo o software con funcionalidad mixta (antivirus, cortafuegos y otras), como un UTM que permite gestionar de manera unificada la mayoría de ciber amenazas que pueden afectar a una empresa.

El uso combinado de estos elementos, que pueden ser tanto software como hardware, y su correcta configuración, reducirá las posibilidades de sufrir un ataque de denegación de servicio.

Medidas de protección en el hosting

En caso de que se haya contratado un hosting debes informarte sobre las medidas de seguridad que ha implementado el proveedor. Tendrás que comprobar que son como las del apartado anterior. Algunos proveedores ofrecen estas medidas de seguridad en el panel de administración del alojamiento web. Verifica con el proveedor quién será el encargado de su configuración y administración.

Ancho de banda

Esta puede que sea la forma de protección más básica, pero no por ello la menos eficaz. Independientemente de que el servicio web se encuentre dentro de la organización o subcontratado se ha de contar con el mayor ancho de banda posible. De esta forma, se podrán gestionar mejor los picos de tráfico que causan las denegaciones de servicio.

Redundancia y balance de carga

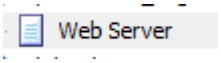
La redundancia consiste en tener el activo duplicado en más de un servidor y el balanceado de carga permite que se asigne a un servidor u otro en función de la carga de trabajo que esté soportando. Esta medida reduce los riesgos de sufrir uno de estos ataques, ya que al tener más de un servidor se reducirá la posibilidad de que se detenga debido a la sobrecarga. Además, aporta otras ventajas como la tolerancia a los fallos, ya que, si un servidor cae, el total del trabajo lo asumiría el otro servidor.

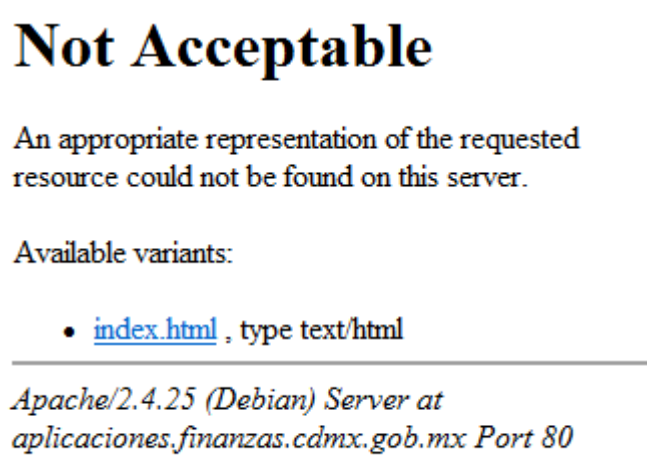
Vulnerabilidades bajas

Apache mod_negotiation filename bruteforcing

mod_negotiation es un módulo de Apache responsable de seleccionar el documento que mejor se adapta a las capacidades del cliente, de uno de varios documentos disponibles. Si el cliente proporciona un encabezado de aceptación no válido, el servidor responderá con un error 406 No aceptable que contiene una lista de pseudo directorio. Este comportamiento puede ayudar a un atacante a aprender más sobre su objetivo, por ejemplo, generar una lista de nombres base, generar una lista de extensiones interesantes, buscar archivos de respaldo, etc.

Afecta a:





Not Acceptable

An appropriate representation of the requested resource could not be found on this server.

Available variants:

- index.html , type text/html

Apache/2.4.25 (Debian) Server at aplicaciones.finanzas.cdmx.gob.mx Port 80

El impacto de esta vulnerabilidad

Posible divulgación de información: lista de directorios, fuerza bruta de nombre de archivo, archivos de respaldo.

Cómo solucionar esta vulnerabilidad

Deshabilite la directiva MultiViews del archivo de configuración de Apache y reinicie Apache.

Puede desactivar MultiViews creando un archivo .htaccess que contenga la siguiente línea:

```
Options -Multiviews
```

Clickjacking: X-Frame-Options header missing

Descripción de la vulnerabilidad

Clickjacking (ataque de reparación de la interfaz de usuario, ataque de reparación de la interfaz de usuario, reparación de la interfaz de usuario) es una técnica maliciosa para engañar a un usuario web para que haga clic en algo diferente de lo que el usuario percibe que está haciendo, revelando así potencialmente información confidencial o tomando el control de su computadora mientras haciendo clic en páginas web aparentemente inocuas.

El servidor no devolvió un encabezado X-Frame-Options, lo que significa que este sitio web podría estar en riesgo de un ataque de clickjacking. El encabezado de respuesta HTTP X-Frame-Options se puede usar para indicar si un navegador debe poder representar una página dentro de un marco o iframe. Los sitios pueden usar esto para evitar ataques de secuestro de clics, asegurándose de que su contenido no esté incrustado en otros sitios.

Afecta a:

Web Server

Cómo solucionar esta vulnerabilidad

Configure su servidor web para incluir un encabezado X-Frame-Options.

Existen tres posibles directivas para X-Frame-Options:

```
X-Frame-Options: DENY
X-Frame-Options: SAMEORIGIN
X-Frame-Options: ALLOW-FROM https://example.com/
```

Si especifica DENY, fallarán no sólo los intentos de cargar la página en un marco desde otros sitios, sino que fallarán cuando sea cargada desde el mismo sitio. Por otro lado, si especifica SAMEORIGIN, puede usar la página en un marco mientras el sitio que la incluya sea el mismo que la sirve.

DENY

La página no puede ser mostrada en un marco, independiente del sitio que esté intentándolo.

SAMEORIGIN

La página sólo puede ser mostrada en un marco del mismo origen que dicha página.

ALLOW-FROM *uri*

La página sólo puede ser mostrada en un marco del origen especificado.Tenga en cuenta que en Firefox esto todavía sufre del mismo problema que SAMEORIGIN — no verifica los antecesores del marco para ver si están en el mismo origen.

Configurar apache ya que esto es a nivel servidor, una ves aplicando esto en el servidor, ningún sistema alojado en el mismo volverá a ser vulnerable a esta alerta.

```
Header always append X-Frame-Options SAMEORIGIN
```

Para que Apache envíe `X-Frame-Options` deny , agregue lo siguiente a la configuración de su sitio:

```
Header set X-Frame-Options DENY
```

Para que Apache envíe el encabezado `X-Frame-Options` para permitir (`ALLOW-FROM`) un host en específico, agregue esto a la configuración de su sitio:

```
Header set X-Frame-Options "ALLOW-FROM https://example.com/"
```

Si usted utiliza apache la opción a elegir es la primera

Header always append X-Frame-Optios SAMEORIGIN

Edite el archivo de configuración de Apache en función de su sistema operativo. El archivo de configuración se puede encontrar:

Sistemas basados en Debian:

/etc/apache2/conf-enabled/security.conf
Sistemas basados en Redhat:

/etc/httpd/conf/httpd.conf

Ahora agregue una de las siguientes entradas al archivo:

Header always append X-Frame-Optios SAMEORIGIN

Una vez realizado reiniciar el servicio apache

Para configurar nginx a que envíe el encabezado X-Frame-Options , agregue esto a la

```
add_header X-Frame-Options SAMEORIGIN;
```

Configurar X-Frame-Options con .htaccess

Los sitios web que se ejecutan a través del entorno de alojamiento compartido, Es posible que no tenga privilegios para modificar la configuración de Apache. En este caso, puede crear el archivo .htaccess en la raíz del documento y anexar

Header always append X-Frame-Optios SAMEORIGIN

ELABORO	VISTO BUENO
ULISES A. CARRANZA MARTÍNEZ	ANTONIO GARCÍA MORALES
JUD DE SEGURIDAD INFORMÁTICA	COORDINADOR DE CALIDAD Y SEGURIDAD INFORMÁTICA