Reporte de Seguridad sitio https://vpsamvc.azurewebsites.net Municipio de Villa Parque Santa Ana

Reporte de seguridad Testing Owasp Top Ten

Descripción:

El presente reporte ejecutivo se realiza en base al estándar de seguridad verificando que el sistema posee valores aceptables de alertas vulneraribilidades definidos en base al acuerdo con el equipo de desarrollo en un margen menor a 5 criticas y 20 de alta calificación. No se incluyen las alertas de información ya que únicamente se utiliza la codificación base 64 y en este caso no exponen nformacion confidencial.

Summary of Alerts

Risk Level	Number of Alerts
<u>High</u>	1
<u>Medium</u>	17
Low	193
<u>Informational</u>	110

Alert Detail

High (Medium)	Escáner de los dispositivos electrónicos Anti CSRF
Description	Una solicutud falsa entre sitios en un ataque que compromete y obliga a una víctima a enviar su solicitud HTTP a un destino objetivo sin su conocimiento o intención para poder realizar una acción como víctima. La causa oculta es la funcionalidad de la aplicación utilizando acciones de URL/formulario que pueden ser adivinados de forma repetible. La naturaleza del ataque es que CSRG explota la confianza que un sitio web proporciona a un usuario. Por el contrario, las cadenas de comandos de los sitios cruzados (XSS) explotan la confianza que un usuario proporciona en un sitio web. Al igual que XSS, los ataques CSRG no son de forma necesaria de sitios cruzados, pero hay la posibilidad de que si pueden serlo. La falsificación de las solicitudes ente los sitios también se conoce como CSRF, XSRG, ataques con un solo clic, montaje de sesión, diputado confundido y navegación en alta mar. Los ataques de CSRG son muy efectivos en varias situaciones, que incluyen:
	*La victima tiene una sesión activa en el sitio de destino.
	*La víctima se autoriza por medio de la autenticación HTTP en el sitio de destino.
	*La víctima se encuentra en la misma red local que el sitio de destino.
	CSRF se ha utilizado especialmente para poder realizar una acción contra un sitio objetivo utilizando los privilegios de la víctima, pero se han revelado técnicas recientes para difundir información al obtener el acceso a la respuesta. El riesgo de divulgación de información

	aumenta de forma drástica cuando el sitio de destino se encuentra vulnerable a XSS, porque XSS se puede utilizar como una plataforma para CSRF, lo que le permite al atacante que opere desde adentro de los líites de la misma política de origen.
Solution	Frase: Arquitectura y Diseño
	Utilice una biblioteca o marco comprobado que no acepte que ocura esta debilidad o que proporcione construcciones que permitan que esta debilidad sea mas sencilla de evitar.
	Por ejemplo, utilice el paquete anti-CSRG como el CSRGuard de OWASP.
	Fase: Implementación
	Asegúrese de que su aplicación esté libre de fallas de secuencias de comandos entre sitios, ya que la mayoría de las defensas de CSRF pueden detenerse por alto por medio del uso de secuencias de comandos manejadas por el atacante.
	Fase: Arquitectura y Diseño
	Origina un nonce único para cada uno de los formularios, coloque el nonce en el formularo y confirme la independencia al obtener el formulario. Asegúrese de que el nonce no sea predecible (CWE-330).
	Usted tiene que tener en cuenta que esto puede pasar desapercibido utilizando XSS.
	Identificar las operaciones que sean especialmente peligrosas. Cuando el usuario desarrolla una operación peligrosa, envíe una solicitud de confirmación de forma separada para poder garantizar que el usuario tenga la intención de desarrollar esa operación.
	Usted tiene que tener en cuenta que esto puede pasar desapercibido utilizando XSS.
	Utilice el control de gestión de la sesión de ESAPI.
	Este control introduce un elemento para CSRF.
	No utilice el método GET para ninguna de las solicitudes que puedan desencadenar un cambio de estado.
	Fase: Implementación
	Revise que la solicitud se creó en la página esperada. Esto podría quebrar la funcionalidad auténtica, ya que los usuarios o los representantes puede ser que hayan desactivado el envío de Referer por motivos de privacidad.
Reference	http://projects.webappsec.org/Cross-Site-Request-Forgery
	http://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
URL	https://vpsamvc.azurewebsites.net/Denuncias/View
Medium (Medium)	Encabezado X-Frame-Options no establecido
Description	El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'.
Solution	Los navegadores de web mas modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte

	de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Denuncias/View
Parameter	X-Frame-Options
Medium (Medium)	Encabezado X-Frame-Options no establecido
Description	El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'.
Solution	Los navegadores de web mas modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Home
Parameter	X-Frame-Options
Medium (Medium)	Encabezado X-Frame-Options no establecido
Description	El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'.
Solution	Los navegadores de web mas modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Account
Parameter	X-Frame-Options
Medium (Medium)	Proxy Disclosure
Description	2 proxy server(s) were detected or fingerprinted. This information helps a potential attacker to determineA list of targets for an attack against the application.
	- Potential vulnerabilities on the proxy servers that service the application.

Disable the 'OPTIONS' method on the proxy servers, as well as the origin web/application server, if it is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing). Configure the web and application servers with custom error pages, to prevent 'fingerprintable product-specific error pages being leaked to the user in the event of HTTP errors, such as TRACK requests for non-existent pages. Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By HTTP response headers. Other Information Intps://tools.ieff.org/html/rfc7231#section-5.1.2 CWE Id 200 WASC Id 45 URL https://bysamvc.azurewebsites.net/Denuncias/Create Attack TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method. Medium (Medium) Proxy Disclosure Description 2 proxy server(s) were detected or fingerprinted. This information helps a potential attacker to determine - A list of targets for an attack against the application. - Potential vulnerabilities on the proxy servers that service the application. - Potential vulnerabilities on the proxy servers has service the application. - The presence or absence of any proxy-based components that might cause attacks against the application to be detected, prevented, or miligated. Solution Disable the 'TRACE' method on the proxy servers, as well as the origin web/application server. If it is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing). Configure the web and application servers with custom error pages, to prevent 'lingerprintable product-specific error pages being leaked to the user in the event of HTTP errors, such as TRACK requests for non-existent pages. Configure all proxies, application servers with custom error pages, to pr		
server, if it is not required for other purposes, such as 'CORS' (Cross Örigin Resource Sharing). Configure the web and application servers with custom error pages, to prevent 'fingerprintable product-specific error pages being leaked to the user in the event of HTTP errors, such as TRACK' requests for non-existent pages. Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers. Other Information Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0/ASP.NET] Reference https://tools.ietf.org/html/rfc7231#section-5.1.2 CWE Id 200 WASC Id 45 URL https://typsamvc.azurewebsites.net/Denuncias/Create Attack TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method. Medium (Medium) Proxy Disclosure Description 2 proxy server(s) were detected or fingerprinted. This information helps a potential attacker to determine - A list of targets for an attack against the application. - Potential vulnerabilities on the proxy servers that service the application. - The presence or absence of any proxy-based components that might cause attacks against the application to be detected, prevented, or mitigated. Solution Disable the "CPTIONS" method on the proxy servers, as well as the origin web/application server, if it is not required for other purposes, such as "CORS" (Cross Origin Resource Sharing). Configure the web and application servers with custom error pages, to prevent 'fingerprintable product-specific error pages being leaked to the user in the event of HTTP errors, such as TRACK requests for non-existent pages. Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response	Solution	Disable the 'TRACE' method on the proxy servers, as well as the origin web/application server.
product-specific error pages being leaked to the user in the event of HTTP errors, such as 'TRACK' requests for non-existent pages. Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By HTTP response headers. Other Information Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0 The following web/application server has been identified between the service service the application. Potential vulnerabilities on the proxy servers that service the application. - Potential vulnerabilities on the proxy servers that service the application. - The presence or absence of any proxy-based components that might cause attacks against the application to be detected, prevented, or mitigated. Solution Disable the 'TRACE' method on the proxy servers, as well as the origin web/application server, if it is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing). Configure the web and application servers with custom error pages, to prevent 'fingerprintable product-specific error pages being leaked to the user in the event of HTTP errors, such as 'TRACK' requests for non-existent pages. Configure all proxies, application servers, and web servers to prevent di		server, if it is not required for other purposes, such as 'CORS' (Cross Origin Resource
technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers. Other Information Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0 The following web/application-server has been identified: - Microsoft-IIS/10.0 (ASP.NET) Reference https://tools.ietf.org/html/rfc7231#section-5.1.2 CWE Id 20 WASC Id 45 URL https://vpsamvc.azurewebsites.net/Denuncias/Create Attack TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method. Medium (Medium) Proxy Disclosure Description 2 proxy server(s) were detected or fingerprinted. This information helps a potential attacker to determine - A list of targets for an attack against the application. - Potential vulnerabilities on the proxy servers that service the application. - The presence or absence of any proxy-based components that might cause attacks against the application to be detected, prevented, or mitigated. Solution Disable the 'TRACE' method on the proxy servers, as well as the origin web/application server, if it is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing). Configure the web and application servers with custom error pages, to prevent 'fingerprintable product-specific error pages being leaked to the user in the event of HTTP errors, such as 'TRACK' requests for non-existent pages. Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers. Other Information Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0 The following web/application server has been identifi		
identified between OWASP ZAP and the application/web server: ** Unknown - Microsoft-IIS/10.0[ASP-NET] Reference https://tools.ietf.org/html/rfc7231#section-5.1.2 CWE Id 200 WASC Id 45 URL https://typsamvc.azurewebsites.net/Denuncias/Create Attack TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method. Medium (Medium) Proxy Disclosure Description 2 proxy server(s) were detected or fingerprinted. This information helps a potential attacker to determine - A list of targets for an attack against the application. - Potential vulnerabilities on the proxy servers that service the application. - The presence or absence of any proxy-based components that might cause attacks against the application to be detected, prevented, or mitigated. Solution Disable the 'TRACE' method on the proxy servers, as well as the origin web/application server, if it is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing). Configure the web and application servers with custom error pages, to prevent 'fingerprintable product-specific error pages being leaked to the user in the event of HTTP errors, such as 'TRACK' requests for non-existent pages. Configure all proxies, application servers and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers. Other Information Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.1 The following veb/application server has been identified: - Microsoft-IIS/10.1 The following veb/application server has been identified: - Microsoft-IIS/10.0 The following veb/application server has been identified: - Microsoft-IIS/10.0 The following veb/application server has been identified: - Microsoft-IIS/10.0 The following veb/application server has been identified: - Microsoft-IIS/10.0 The following v		technology and version information in the 'Server' and 'X-Powered-By' HTTP response
CWE Id WASC Id 45 URL https://vpsamvc.azurewebsites.net/Denuncias/Create Attack TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method. Medium (Medium) Proxy Disclosure Description 2 proxy server(s) were detected or fingerprinted. This information helps a potential attacker to determine - A list of targets for an attack against the application Potential vulnerabilities on the proxy servers that service the application The presence or absence of any proxy-based components that might cause attacks against the application to be detected, prevented, or mitigated. Solution Disable the 'TRACE' method on the proxy servers, as well as the origin web/application server, if it is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing). Configure the web and application servers with custom error pages, to prevent 'fingerprintable product-specific error pages being leaked to the user in the event of HTTP errors, such as 'TRACK' requests for non-existent pages. Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers. Other Information Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0 The following web/application-5.1.2 CWE Id 200 WASC Id 45	Other Information	identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-
WASC Id URL https://vpsamvc.azurewebsites.net/Denuncias/Create Attack TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method. Medium (Medium) Proxy Disclosure Description 2 proxy server(s) were detected or fingerprinted. This information helps a potential attacker to determine - A list of targets for an attack against the application. - Potential vulnerabilities on the proxy servers that service the application. - The presence or absence of any proxy-based components that might cause attacks against the application to be detected, prevented, or mitigated. Solution Disable the 'TRACE' method on the proxy servers, as well as the origin web/application server, if it is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing). Configure the web and application servers with custom error pages, to prevent 'fingerprintable product-specific error pages being leaked to the user in the event of HTTP errors, such as 'TRACK' requests for non-existent pages. Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers. Other Information Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0[ASP.NET] Reference https://tools.ietf.org/html/rfc7231#section-5.1.2 CWE Id 200 WASC Id 45	Reference	https://tools.ietf.org/html/rfc7231#section-5.1.2
Attack TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method. Medium (Medium) Proxy Disclosure Description 2 proxy server(s) were detected or fingerprinted. This information helps a potential attacker to determine - A list of targets for an attack against the application. - Potential vulnerabilities on the proxy servers that service the application. - The presence or absence of any proxy-based components that might cause attacks against the application to be detected, prevented, or mitigated. Solution Disable the 'TRACE' method on the proxy servers, as well as the origin web/application server, if it is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing). Configure the web and application servers with custom error pages, to prevent 'fingerprintable product-specific error pages being leaked to the user in the event of HTTP errors, such as TRACK' requests for non-existent pages. Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers. Other Information Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0[ASP.NET] Reference https://tools.ietf.org/html/rfc7231#section-5.1.2 CWE Id 200 WASC Id 45	CWE Id	200
Attack TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method. Medium (Medium) Proxy Disclosure Description 2 proxy server(s) were detected or fingerprinted. This information helps a potential attacker to determine - A list of targets for an attack against the application. - Potential vulnerabilities on the proxy servers that service the application. - The presence or absence of any proxy-based components that might cause attacks against the application to be detected, prevented, or mitigated. Solution Disable the 'TRACE' method on the proxy servers, as well as the origin web/application server, if it is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing). Configure the web and application servers with custom error pages, to prevent 'fingerprintable product-specific error pages being leaked to the user in the event of HTTP errors, such as 'TRACK' requests for non-existent pages. Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers. Other Information Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0[ASP.NET] Reference https://tools.ietf.org/html/rfc7231#section-5.1.2 CWE Id 200 WASC Id	WASC Id	45
Description 2 proxy server(s) were detected or fingerprinted. This information helps a potential attacker to determine - A list of targets for an attack against the application. - Potential vulnerabilities on the proxy servers that service the application. - The presence or absence of any proxy-based components that might cause attacks against the application to be detected, prevented, or mitigated. Solution Disable the 'TRACE' method on the proxy servers, as well as the origin web/application server. Disable the 'OPTIONS' method on the proxy servers, as well as the origin web/application server, if it is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing). Configure the web and application servers with custom error pages, to prevent 'fingerprintable product-specific error pages being leaked to the user in the event of HTTP errors, such as 'TRACK' requests for non-existent pages. Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers. Other Information Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0 [ASP.NET] Reference https://tools.ietf.org/html/rfc7231#section-5.1.2 CWE Id 200 WASC Id 45	URL	https://vpsamvc.azurewebsites.net/Denuncias/Create
Description 2 proxy server(s) were detected or fingerprinted. This information helps a potential attacker to determine - A list of targets for an attack against the application. - Potential vulnerabilities on the proxy servers that service the application. - The presence or absence of any proxy-based components that might cause attacks against the application to be detected, prevented, or mitigated. Solution Disable the 'TRACE' method on the proxy servers, as well as the origin web/application server. If it is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing). Configure the web and application servers with custom error pages, to prevent 'fingerprintable product-specific error pages being leaked to the user in the event of HTTP errors, such as 'TRACK' requests for non-existent pages. Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers. Other Information Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 [ASP.NET] Reference https://tools.ietf.org/html/rfc7231#section-5.1.2 CWE Id 200 WASC Id 45	Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
determine - A list of targets for an attack against the application. - Potential vulnerabilities on the proxy servers that service the application. - The presence or absence of any proxy-based components that might cause attacks against the application to be detected, prevented, or mitigated. Solution Disable the 'TRACE' method on the proxy servers, as well as the origin web/application server. It is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing). Configure the web and application servers with custom error pages, to prevent 'fingerprintable product-specific error pages being leaked to the user in the event of HTTP errors, such as TRACK' requests for non-existent pages. Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers. Other Information Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 [ASP.NET] Reference https://tools.ietf.org/html/rfc7231#section-5.1.2 CWE Id WASC Id determine the application.	Medium (Medium)	Proxy Disclosure
- Potential vulnerabilities on the proxy servers that service the application. - The presence or absence of any proxy-based components that might cause attacks against the application to be detected, prevented, or mitigated. Solution Disable the 'TRACE' method on the proxy servers, as well as the origin web/application server. Disable the 'OPTIONS' method on the proxy servers, as well as the origin web/application server, if it is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing). Configure the web and application servers with custom error pages, to prevent 'fingerprintable product-specific error pages being leaked to the user in the event of HTTP errors, such as 'TRACK' requests for non-existent pages. Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers. Other Information Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0[ASP.NET] Reference https://tools.ietf.org/html/rfc7231#section-5.1.2 CWE Id 200 WASC Id	Description	
- The presence or absence of any proxy-based components that might cause attacks against the application to be detected, prevented, or mitigated. Solution Disable the 'TRACE' method on the proxy servers, as well as the origin web/application server. Disable the 'OPTIONS' method on the proxy servers, as well as the origin web/application server, if it is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing). Configure the web and application servers with custom error pages, to prevent 'fingerprintable product-specific error pages being leaked to the user in the event of HTTP errors, such as 'TRACK' requests for non-existent pages. Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers. Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0[ASP.NET] Reference https://tools.ietf.org/html/rfc7231#section-5.1.2 CWE Id WASC Id 45		- A list of targets for an attack against the application.
the application to be detected, prevented, or mitigated. Solution Disable the 'TRACE' method on the proxy servers, as well as the origin web/application server. Disable the 'OPTIONS' method on the proxy servers, as well as the origin web/application server, if it is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing). Configure the web and application servers with custom error pages, to prevent 'fingerprintable product-specific error pages being leaked to the user in the event of HTTP errors, such as 'TRACK' requests for non-existent pages. Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers. Other Information Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0[ASP.NET] Reference https://tools.ietf.org/html/rfc7231#section-5.1.2 CWE Id 200 WASC Id		- Potential vulnerabilities on the proxy servers that service the application.
Disable the 'OPTIONS' method on the proxy servers, as well as the origin web/application server, if it is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing). Configure the web and application servers with custom error pages, to prevent 'fingerprintable product-specific error pages being leaked to the user in the event of HTTP errors, such as 'TRACK' requests for non-existent pages. Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers. Other Information Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0[ASP.NET] Reference https://tools.ietf.org/html/rfc7231#section-5.1.2 CWE Id 200 WASC Id		
server, if it is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing). Configure the web and application servers with custom error pages, to prevent 'fingerprintable product-specific error pages being leaked to the user in the event of HTTP errors, such as 'TRACK' requests for non-existent pages. Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers. Other Information Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0[ASP.NET] Reference https://tools.ietf.org/html/rfc7231#section-5.1.2 CWE Id 200 WASC Id	Solution	Disable the 'TRACE' method on the proxy servers, as well as the origin web/application server.
product-specific error pages being leaked to the user in the event of HTTP errors, such as 'TRACK' requests for non-existent pages. Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers. Other Information Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0[ASP.NET] Reference https://tools.ietf.org/html/rfc7231#section-5.1.2 CWE Id 200 WASC Id		server, if it is not required for other purposes, such as 'CORS' (Cross Origin Resource
technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers. Other Information Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0[ASP.NET] Reference https://tools.ietf.org/html/rfc7231#section-5.1.2 CWE Id WASC Id 45		
identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0[ASP.NET] Reference https://tools.ietf.org/html/rfc7231#section-5.1.2 CWE Id 200 WASC Id 45		technology and version information in the 'Server' and 'X-Powered-By' HTTP response
Reference https://tools.ietf.org/html/rfc7231#section-5.1.2 CWE Id 200 WASC Id 45	Other Information	identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-
CWE Id 200 WASC Id 45	Reference	
WASC Id 45		
UNL https://vpsainvc.azurewebsites.net/Denuncias/Create	URL	https://vpsamvc.azurewebsites.net/Denuncias/Create

Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
Medium (Medium)	Encabezado X-Frame-Options no establecido
Description	El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'.
Solution	Los navegadores de web mas modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Account/Login
Parameter	X-Frame-Options
Modium (Modium)	Durana Dia dia any
Medium (Medium)	
Description	2 proxy server(s) were detected or fingerprinted. This information helps a potential attacker to determine
	- A list of targets for an attack against the application.
	- Potential vulnerabilities on the proxy servers that service the application.
	- The presence or absence of any proxy-based components that might cause attacks against the application to be detected, prevented, or mitigated.
Solution	Disable the 'TRACE' method on the proxy servers, as well as the origin web/application server.
	Disable the 'OPTIONS' method on the proxy servers, as well as the origin web/application server, if it is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing).
	Configure the web and application servers with custom error pages, to prevent 'fingerprintable' product-specific error pages being leaked to the user in the event of HTTP errors, such as 'TRACK' requests for non-existent pages.
	Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers.
Other Information	Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0[ASP.NET]
Reference	https://tools.ietf.org/html/rfc7231#section-5.1.2
CWE Id	200
WASC Id	45
URL	https://vpsamvc.azurewebsites.net/Denuncias
Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
Medium (Medium)	Vulnerable JS Library
Description	The identified library jquery, version 3.3.1 is vulnerable.

Solution	
	Please upgrade to the latest version of jquery.
Other Information	CVE-2019-11358
Reference	https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/
	https://nvd.nist.gov/vuln/detail/CVE-2019-11358
	https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b
	https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
CWE Id	829
URL	https://vpsamvc.azurewebsites.net/lib/jquery/dist/jquery.min.js
Medium (Medium)	Encabezado X-Frame-Options no establecido
Description	El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'.
Solution	Los navegadores de web mas modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Account/Register
Parameter	X-Frame-Options
Medium (Medium)	Encabezado X-Frame-Options no establecido
Description	El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'.
Description Solution	El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante
	El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'. Los navegadores de web mas modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios
Solution	El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'. Los navegadores de web mas modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles). http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-
Solution	El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'. Los navegadores de web mas modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles). http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
Solution Reference CWE Id	El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'. Los navegadores de web mas modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles). http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
Solution Reference CWE Id WASC Id	El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'. Los navegadores de web mas modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles). http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx 16
Solution Reference CWE Id WASC Id URL	El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'. Los navegadores de web mas modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles). http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx 16 15 https://vpsamvc.azurewebsites.net/Account/Login X-Frame-Options
Solution Reference CWE Id WASC Id URL Parameter	El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'. Los navegadores de web mas modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles). http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx 16 15 https://vpsamvc.azurewebsites.net/Account/Login X-Frame-Options
Solution Reference CWE Id WASC Id URL Parameter Medium (Medium)	El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'. Los navegadores de web mas modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles). http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx 16 15 https://vpsamvc.azurewebsites.net/Account/Login X-Frame-Options Proxy Disclosure 2 proxy server(s) were detected or fingerprinted. This information helps a potential attacker to

	- The presence or absence of any proxy-based components that might cause attacks against the application to be detected, prevented, or mitigated.
Solution	Disable the 'TRACE' method on the proxy servers, as well as the origin web/application server.
	Disable the 'OPTIONS' method on the proxy servers, as well as the origin web/application server, if it is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing).
	Configure the web and application servers with custom error pages, to prevent 'fingerprintable' product-specific error pages being leaked to the user in the event of HTTP errors, such as 'TRACK' requests for non-existent pages.
	Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers.
Other Information	Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0[ASP.NET]
Reference	https://tools.ietf.org/html/rfc7231#section-5.1.2
CWE Id	200
WASC Id	45
URL	https://vpsamvc.azurewebsites.net/Denuncias/View
Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
Medium (Medium)	Encabezado X-Frame-Options no establecido
Description	El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'.
Solution	Los navegadores de web mas modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/denuncias/create
Parameter	X-Frame-Options
Medium (Medium)	Proxy Disclosure
Description	2 proxy server(s) were detected or fingerprinted. This information helps a potential attacker to determine
	- A list of targets for an attack against the application.
	- Potential vulnerabilities on the proxy servers that service the application.
	- The presence or absence of any proxy-based components that might cause attacks against the application to be detected, prevented, or mitigated.
Solution	Disable the 'TRACE' method on the proxy servers, as well as the origin web/application server.

	Disable the 'OPTIONS' method on the proxy servers, as well as the origin web/application server, if it is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing).
	Configure the web and application servers with custom error pages, to prevent 'fingerprintable' product-specific error pages being leaked to the user in the event of HTTP errors, such as 'TRACK' requests for non-existent pages.
	Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers.
Other Information	Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0[ASP.NET]
Reference	https://tools.ietf.org/html/rfc7231#section-5.1.2
CWE Id	200
WASC Id	45
URL	https://vpsamvc.azurewebsites.net/Denuncias/View
Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
Medium (Medium)	Encabezado X-Frame-Options no establecido
Description	El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'.
Solution	Los navegadores de web mas modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Account/Register
Parameter	X-Frame-Options
Medium (Medium)	Encabezado X-Frame-Options no establecido
Description	El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'.
Solution	Los navegadores de web mas modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Denuncias/Create
Parameter	X-Frame-Options

Medium	(Medium)	Encabezado X-Frame-Options no establecido		
Description				
Solution		Los navegadores de web mas modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles).		
Reference		http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx		
CWE Id		16		
WASC Id		15		
URL	ļ	https://vpsamvc.azurewebsites.net/Denuncias/Create		
Parameter		X-Frame-Options		
Medium				
(Medium	Proxy Dis	closure		
)				
Description	2 proxy serve	er(s) were detected or fingerprinted. This information helps a potential attacker to determine		
	- A list of targ	gets for an attack against the application.		
	- Potential vu	ulnerabilities on the proxy servers that service the application.		
	- The presence or absence of any proxy-based components that might cause attacks against the application to be detected, prevented, or mitigated.			
Solution	Disable the "	TRACE' method on the proxy servers, as well as the origin web/application server.		
		OPTIONS' method on the proxy servers, as well as the origin web/application server, if it is not other purposes, such as 'CORS' (Cross Origin Resource Sharing).		
		e web and application servers with custom error pages, to prevent 'fingerprintable' product- r pages being leaked to the user in the event of HTTP errors, such as 'TRACK' requests for pages.		
		I proxies, application servers, and web servers to prevent disclosure of the technology and mation in the 'Server' and 'X-Powered-By' HTTP response headers.		
Other Information	Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown - Microsoft-IIS/10.0 The following web/application server has been identified: - Microsoft-IIS/10.0[ASP.NET]			
Reference				
CWE Id	200			
WASC Id	45			
URL	https://vpsamvc.azurewebsites.net/Denuncias/View?Denunciald&Descripcion&EstadoDenunciald&UserId			
Attack	TRACE, OP	TIONS methods with 'Max-Forwards' header. TRACK method.		
Low (Hig	,	Server Leaks Version Information via "Server" HTTP Response Header Field		
Description	ŀ	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.		

Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/img/Candado.png
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
OWELL	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id URL	13
	https://vpsamvc.azurewebsites.net/denuncias/create
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/lib/bootstrap/dist/js/bootstrap.bundle.min.js

Low	Ctrict T	romaniant Consumity Handon Not Cot
(High)	Strict-11	ransport-Security Header Not Set
Descriptio n	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.	
Solution	Ensure that Transport	at your web server, application server, load balancer, etc. is configured to enforce StrictSecurity.
Reference	https://che	eatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	https://owa	asp.org/www-community/Security_Headers
	http://en.w	vikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://cani	use.com/stricttransportsecurity
	http://tools	s.ietf.org/html/rfc6797
CWE Id	16	
WASC Id	15	
URL	https://vp 0	samvc.azurewebsites.net/js/site.js?v=4q1jwFhaPaZgr8WAUSrux6hAuh0XDg9kPS3xIVq36I
Low (Hig	ıh)	Server Leaks Version Information via "Server" HTTP Response Header
		Field
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.
Solution		Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference		http://httpd.apache.org/docs/current/mod/core.html#servertokens
		http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
		http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
		http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id		200
WASC Id		13
URL		https://vpsamvc.azurewebsites.net/lib/jquery-validation- unobtrusive/jquery.validate.unobtrusive.min.js
Low (Hig	ıh) Stı	rict-Transport-Security Header Not Set
declares that complying user agents (such as a web browser) are secure HTTPS connections (i.e. HTTP layered over TLS/SSL). He		TP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server clares that complying user agents (such as a web browser) are to interact with it using only cure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track stocol and is specified in RFC 6797.
Solution		sure that your web server, application server, load balancer, etc. is configured to enforce Strict- ansport-Security.
Reference	http	os://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
ř		os://owasp.org/www-community/Security_Headers

	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/img/Candado.png
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/lib/bootstrap/dist/css/bootstrap.min.css
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	$https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html$
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Denuncias/Create
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/lib/jquery-validation- unobtrusive/jquery.validate.unobtrusive.min.js
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Denuncias/Create
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/lib/jquery-validation/dist/jquery.validate.min.js

Low (High)	Server Leaks Version Information via "Server" HTTP Response Header Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Account/Register
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header
	Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Account/Register
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200

WASC Id		13
URL		https://vpsamvc.azurewebsites.net/lib/toastr/toastr.min.css
Low (Hig	ıh)	Server Leaks Version Information via "Server" HTTP Response Header Field
Description	ľ	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.
Solution		Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference		http://httpd.apache.org/docs/current/mod/core.html#servertokens
		http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
		http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
		http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id		200
WASC Id		13
URL		https://vpsamvc.azurewebsites.net/lib/bootstrap/dist/css/bootstrap.min.css
Low (High)	Serve	r Leaks Version Information via "Server" HTTP Response Header Field
Descriptio n	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.	
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server' header or provide generic details.	
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens	
http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007		sdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blo	ogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
		ww.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200	
WASC Id URL	13	vpsamvc.azurewebsites.net/js/site.js?v=4q1jwFhaPaZgr8WAUSrux6hAuh0XDg9kPS3xIVq36I
OKL	0	vpsamvc.azurewebsites.neujs/site.js:v=+qrjwrnar azgrovvAosruxonAunoAbgski osxivqsor
Low (Hig	jh) g	Strict-Transport-Security Header Not Set
Description	c	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution		Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict- Fransport-Security.
Reference		https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	h	nttps://owasp.org/www-community/Security_Headers
	h	nttp://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security

	Luc Herritana de la California de la Su
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/lib/fontawesome/css/all.min.css
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Denuncias/Create
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track
	protocol and is specified in RFC 6797.
Solution	
Solution Reference	protocol and is specified in RFC 6797. Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-
	protocol and is specified in RFC 6797. Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
	protocol and is specified in RFC 6797. Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security. https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	protocol and is specified in RFC 6797. Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security. https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers
	protocol and is specified in RFC 6797. Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security. https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security http://caniuse.com/stricttransportsecurity
	protocol and is specified in RFC 6797. Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security. https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
Reference	protocol and is specified in RFC 6797. Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security. https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security http://caniuse.com/stricttransportsecurity http://tools.ietf.org/html/rfc6797
Reference CWE Id	protocol and is specified in RFC 6797. Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security. https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security http://caniuse.com/stricttransportsecurity http://tools.ietf.org/html/rfc6797
Reference CWE Id WASC Id	protocol and is specified in RFC 6797. Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security. https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security http://caniuse.com/stricttransportsecurity http://tools.ietf.org/html/rfc6797 16 15
Reference CWE Id WASC Id URL	protocol and is specified in RFC 6797. Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security. https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security http://caniuse.com/stricttransportsecurity http://tools.ietf.org/html/rfc6797 16 15 https://vpsamvc.azurewebsites.net/denuncias/create
CWE Id WASC Id URL Low (High)	protocol and is specified in RFC 6797. Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security. https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security http://caniuse.com/stricttransportsecurity http://tools.ietf.org/html/rfc6797 16 15 https://vpsamvc.azurewebsites.net/denuncias/create Strict-Transport-Security Header Not Set HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track

Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/sitemap.xml
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/img/VPSA.png
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/lib/jquery-validation/dist/jquery.validate.min.js

Low (High)	Server Leaks Version Information via "Server" HTTP Response Header Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Denuncias
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Account/Login
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security

	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/lib/Datatables/datatables.min.js
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Account/Login
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/img/VPSA.png
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
Reference	The strategic and the strategi
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Account
Low (High)	Strict-Transport-Security Header Not Set
, , ,	
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Account/Register
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header
_e (g,	Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Account/Login
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header Field

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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
OME II	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/sitemap.xml
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/favicon.ico
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	$https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html$
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15

URL I	https://vpsamvc.azurewebsites.net/img/reclamos.jpg
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/lib/Datatables/datatables.min.js
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/img/Obras.jpg
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Account/Login
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	$https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html$
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Account/Register
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
OME	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id WASC Id	200 13
URL	https://vpsamvc.azurewebsites.net/css/site.css
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	https://owasp.org/www-community/Security_Headers

	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
	16
	15
	https://vpsamvc.azurewebsites.net/Denuncias/View
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Denuncias/View
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header
Low (High)	
Low (High) Description	Server Leaks Version Information via "Server" HTTP Response Header
, , ,	Server Leaks Version Information via "Server" HTTP Response Header Field 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
Description	Server Leaks Version Information via "Server" HTTP Response Header Field 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. Ensure that your web server, application server, load balancer, etc. is configured to suppress
Description Solution	Server Leaks Version Information via "Server" HTTP Response Header Field 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. Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Description Solution	Server Leaks Version Information via "Server" HTTP Response Header Field 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. Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details. http://httpd.apache.org/docs/current/mod/core.html#servertokens
Description Solution Reference	Server Leaks Version Information via "Server" HTTP Response Header Field 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. Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details. http://httpd.apache.org/docs/current/mod/core.html#servertokens http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
Description Solution Reference	Server Leaks Version Information via "Server" HTTP Response Header Field 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. Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details. http://httpd.apache.org/docs/current/mod/core.html#servertokens http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
Description Solution Reference CWE Id WASC Id	Server Leaks Version Information via "Server" HTTP Response Header Field 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. Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details. http://httpd.apache.org/docs/current/mod/core.html#servertokens http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
Description Solution Reference CWE Id WASC Id URL	Server Leaks Version Information via "Server" HTTP Response Header Field 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. Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details. http://httpd.apache.org/docs/current/mod/core.html#servertokens http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html 200 13 https://vpsamvc.azurewebsites.net/lib/fontawesome/webfonts/fa-solid-900.woff2
Description Solution Reference CWE Id WASC Id	Server Leaks Version Information via "Server" HTTP Response Header Field 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. Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details. http://httpd.apache.org/docs/current/mod/core.html#servertokens http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
Description Solution Reference CWE Id WASC Id URL	Server Leaks Version Information via "Server" HTTP Response Header Field 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. Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details. http://httpd.apache.org/docs/current/mod/core.html#servertokens http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html 200 13 https://vpsamvc.azurewebsites.net/lib/fontawesome/webfonts/fa-solid-900.woff2 Server Leaks Version Information via "Server" HTTP Response Header

CWE Id WASC Id URL Low (High)	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security http://caniuse.com/stricttransportsecurity http://tools.ietf.org/html/rfc6797 16 15 https://vpsamvc.azurewebsites.net/lib/fontawesome/webfonts/fa-solid-900.woff2
WASC Id	http://caniuse.com/stricttransportsecurity http://tools.ietf.org/html/rfc6797 16 15
	http://caniuse.com/stricttransportsecurity http://tools.ietf.org/html/rfc6797 16
	http://caniuse.com/stricttransportsecurity http://tools.ietf.org/html/rfc6797
	http://caniuse.com/stricttransportsecurity
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	https://owasp.org/www-community/Security_Headers
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Low (High)	Strict-Transport-Security Header Not Set
URL	https://vpsamvc.azurewebsites.net/favicon.ico
WASC Id	15
CWE Id	16
	http://caniuse.com/stricttransportsecurity http://tools.ietf.org/html/rfc6797
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	https://owasp.org/www-community/Security_Headers
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Low (High)	Strict-Transport-Security Header Not Set
URL	https://vpsamvc.azurewebsites.net/img/reclamos.jpg
WASC Id	13
CWE Id	200
	headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007

Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/css/site.css
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header
Low (ringil)	Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/lib/Datatables/datatables.min.css
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200

WASC Id URL	13 https://vpsamvc.azurewebsites.net/Denuncias/View
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/robots.txt
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/img/Obras.jpg
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	https://owasp.org/www-community/Security_Headers

	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Denuncias
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Home
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	$https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html$
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Denuncias/View
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Account
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/lib/jquery/dist/jquery.min.js
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15

URL	https://vpsamvc.azurewebsites.net/lib/toastr/toastr.min.js
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security http://caniuse.com/stricttransportsecurity http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/img/DEnuncia_Ciudadana.jpg
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header
Low (High)	Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/img/DEnuncia_Ciudadana.jpg
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx

		http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id		200
WASC Id		13
URL		https://vpsamvc.azurewebsites.net/lib/fontawesome/css/all.min.css
Low (Hig	gh)	Server Leaks Version Information via "Server" HTTP Response Header Field
Description	1	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.
Solution		Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference		http://httpd.apache.org/docs/current/mod/core.html#servertokens
		http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
		http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
		http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id		200
WASC Id		13
URL		https://vpsamvc.azurewebsites.net/lib/toastr/toastr.min.js
Low (Hig	gh)	Server Leaks Version Information via "Server" HTTP Response Header Field
Description	1	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.
Solution		Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference		http://httpd.apache.org/docs/current/mod/core.html#servertokens
		http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
		http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
		http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id		200
WASC Id		13
URL		https://vpsamvc.azurewebsites.net/lib/jquery/dist/jquery.min.js
Low (High)	Strict-Tra	nsport-Security Header Not Set
Descriptio n	that complyi	Transport Security (HSTS) is a web security policy mechanism whereby a web server declares ing user agents (such as a web browser) are to interact with it using only secure HTTPS is (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified 7.
Solution	Ensure that Transport-S	your web server, application server, load balancer, etc. is configured to enforce Strict-ecurity.
Reference	https://cheat	tsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html

	https://	owasp.org/www-community/Security_Headers
	http://e	n.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	11ttp://0	m. m. podia. org. wik., i i i _otroc_i ranoport_occurry
	http://c	aniuse.com/stricttransportsecurity
	http://to	pols.ietf.org/html/rfc6797
CWE Id	16	
WASC Id	15	
URL	https:/ Userld	//vpsamvc.azurewebsites.net/Denuncias/View?Denunciald&Descripcion&EstadoDenunciald&
Low (Hig	gh)	Strict-Transport-Security Header Not Set
Description	1	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution		Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference		https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
		https://owasp.org/www-community/Security_Headers
		http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
		http://caniuse.com/stricttransportsecurity
		http://tools.ietf.org/html/rfc6797
CWE Id		16
WASC Id		15
URL		https://vpsamvc.azurewebsites.net/lib/toastr/toastr.min.css
Low (Hig	gh)	Server Leaks Version Information via "Server" HTTP Response Header Field
Description	1	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.
Solution		Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference		http://httpd.apache.org/docs/current/mod/core.html#servertokens
		http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
		http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
		http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id		200
WASC Id		13
URL		https://vpsamvc.azurewebsites.net/Home
Low (Hig	gh)	Strict-Transport-Security Header Not Set
Description	1	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only

	secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Denuncias/Create
Low (High)	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	$https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html$
	https://owasp.org/www-community/Security_Headers
	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
	http://caniuse.com/stricttransportsecurity
	http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/lib/Datatables/datatables.min.css
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13

URL	https://vpsamvc.azurewebsites.net/lib/bootstrap/dist/js/bootstrap.bundle.min.js
Low (High)	Server Leaks Version Information via "Server" HTTP Response Header Field
Descriptio n	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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Denuncias/View?Denunciald&Descripcion&EstadoDenunciald&UserId
Low (Hig	Jh) Server Leaks Version Information via "Server" HTTP Response Header Field
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens
	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/robots.txt
Low (Me	dium) Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13

URL	https://vpsamvc.azurewebsites.net/lib/Datatables/datatables.min.js
Low (Medium)	Content Security Policy (CSP) Header Not Set
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.
Reference	https://developer.mozilla.org/en- US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
	https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
	http://www.w3.org/TR/CSP/
	http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html
	http://www.html5rocks.com/en/tutorials/security/content-security-policy/
	http://caniuse.com/#feat=contentsecuritypolicy
	http://content-security-policy.com/
CWE Id	16
WASC Id	15
WASC Id URL	
URL	https://vpsamvc.azurewebsites.net/Denuncias/Create
URL	https://vpsamvc.azurewebsites.net/Denuncias/Create Server Leaks Information via "X-Powered-By" HTTP Response Header
URL Low (Medium)	https://vpsamvc.azurewebsites.net/Denuncias/Create Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such
URL Low (Medium) Description	https://vpsamvc.azurewebsites.net/Denuncias/Create Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to. Ensure that your web server, application server, load balancer, etc. is configured to suppress
URL Low (Medium) Description Solution	https://vpsamvc.azurewebsites.net/Denuncias/Create Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to. Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-
URL Low (Medium) Description Solution	https://vpsamvc.azurewebsites.net/Denuncias/Create Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to. Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
URL Low (Medium) Description Solution Reference	https://vpsamvc.azurewebsites.net/Denuncias/Create Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to. Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
URL Low (Medium) Description Solution Reference CWE Id	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to. Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
URL Low (Medium) Description Solution Reference CWE Id WASC Id	https://vpsamvc.azurewebsites.net/Denuncias/Create Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to. Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html 200 13
URL Low (Medium) Description Solution Reference CWE Id WASC Id URL	https://vpsamvc.azurewebsites.net/Denuncias/Create Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to. Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html 200 13 https://vpsamvc.azurewebsites.net/img/VPSA.png
URL Low (Medium) Description Solution Reference CWE Id WASC Id URL Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to. Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html 200 13 https://vpsamvc.azurewebsites.net/img/VPSA.png Cookie Without SameSite Attribute A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter
URL Low (Medium) Description Solution Reference CWE Id WASC Id URL Low (Medium) Description	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to. Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html 200 13 https://vpsamvc.azurewebsites.net/img/VPSA.png Cookie Without SameSite Attribute A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Low (Medium) Description Solution Reference CWE Id WASC Id URL Low (Medium) Description Solution	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to. Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html 200 13 https://vpsamvc.azurewebsites.net/img/VPSA.png Cookie Without SameSite Attribute A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks. Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Account/Register
Parameter	ARRAffinity
Low (Medium)	Feature Policy Header Not Set
Description	Feature Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Feature Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Feature-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy
	https://developers.google.com/web/updates/2018/06/feature-policy
	https://scotthelme.co.uk/a-new-security-header-feature-policy/
	https://w3c.github.io/webappsec-feature-policy/
	https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/lib/jquery/dist/jquery.min.js
Low (Medium)	No se encuentra encabezado X-Content-Type-Options Header
Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.
Solution	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web.
	Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Other Information	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/lib/fontawesome/css/all.min.css
Parameter	X-Content-Type-Options
Low (Medium)	No se encuentra encabezado X-Content-Type-Options Header
Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-

	sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.
Solution	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web.
	Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Other Information	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Account/Login
Parameter	X-Content-Type-Options
Low (Medium)	Content Security Policy (CSP) Header Not Set
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.
Reference	https://developer.mozilla.org/en- US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
	https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
	http://www.w3.org/TR/CSP/
	http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html
	http://www.html5rocks.com/en/tutorials/security/content-security-policy/
	http://caniuse.com/#feat=contentsecuritypolicy
	http://content-security-policy.com/
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Denuncias/Create
Low (Medium)	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma
Description	El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido.

Solution	Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache.
Reference	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
CWE Id	525
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/lib/fontawesome/css/all.min.css
Parameter	Cache-Control
Low (Medium)	Content Security Policy (CSP) Header Not Set
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.
Reference	https://developer.mozilla.org/en- US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
	https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
	http://www.w3.org/TR/CSP/
	http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html
	http://www.html5rocks.com/en/tutorials/security/content-security-policy/
	http://caniuse.com/#feat=contentsecuritypolicy
	http://content-security-policy.com/
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Account/Register
Low (Medium)	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma
Description	El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido.
Solution	Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache.
Reference	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
CWE Id	525
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/lib/toastr/toastr.min.css
Parameter	Cache-Control
Low (Medium)	Content Security Policy (CSP) Header Not Set

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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.
Reference	https://developer.mozilla.org/en- US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
	https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
	http://www.w3.org/TR/CSP/
	http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html
	http://www.html5rocks.com/en/tutorials/security/content-security-policy/
	http://caniuse.com/#feat=contentsecuritypolicy
	http://content-security-policy.com/
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Account/Login
URL <mark>Low (Medium)</mark>	https://vpsamvc.azurewebsites.net/Account/Login Incompleto o no Cache-control y sistema de encabezado HTTP Pragma
Low (Medium)	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o
Low (Medium) Description	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido. Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido
Low (Medium) Description Solution	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido. Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache.
Low (Medium) Description Solution Reference	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido. Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache. https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
Low (Medium) Description Solution Reference CWE Id	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido. Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache. https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching 525
Low (Medium) Description Solution Reference CWE Id WASC Id	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido. Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache. https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching 525
Low (Medium) Description Solution Reference CWE Id WASC Id URL	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido. Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache. https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching 525 13 https://vpsamvc.azurewebsites.net/Account/Login
Low (Medium) Description Solution Reference CWE Id WASC Id URL Parameter	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido. Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache. https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching 525 13 https://vpsamvc.azurewebsites.net/Account/Login Cache-Control
Low (Medium) Description Solution Reference CWE Id WASC Id URL Parameter Low (Medium)	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido. Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache. https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching 525 13 https://vpsamvc.azurewebsites.net/Account/Login Cache-Control No se encuentra encabezado X-Content-Type-Options Header El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán
Low (Medium) Description Solution Reference CWE Id WASC Id URL Parameter Low (Medium) Description	El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido. Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache. https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching 525 13 https://vpsamvc.azurewebsites.net/Account/Login Cache-Control No se encuentra encabezado X-Content-Type-Options Header El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff'

Solution Reference CWE Id WASC Id URL Low (Medium) Description Solution Reference	components may be subject to. Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html 200 13 https://vpsamvc.azurewebsites.net/lib/toastr/toastr.min.js Feature Policy Header Not Set Feature Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Feature Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc. Ensure that your web server, application server, load balancer, etc. is configured to set the Feature-Policy header. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy
Reference CWE Id WASC Id URL Low (Medium) Description	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html 200 13 https://vpsamvc.azurewebsites.net/lib/toastr/toastr.min.js Feature Policy Header Not Set Feature Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Feature Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
Reference CWE Id WASC Id URL Low (Medium)	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html 200 13 https://vpsamvc.azurewebsites.net/lib/toastr/toastr.min.js Feature Policy Header Not Set
Reference CWE Id WASC Id URL	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html 200 13
Reference CWE Id WASC Id	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html 200 13
Reference CWE Id	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
Reference	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress
	components may be subject to.
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
URL	https://vpsamvc.azurewebsites.net/lib/jquery-validation/dist/jquery.validate.min.js
WASC Id	13
CWE Id	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Parameter	X-Content-Type-Options
URL	https://vpsamvc.azurewebsites.net/Account/Login
WASC Id	15
CWE Id	16
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
	a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Other Information	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas

	https://developers.google.com/web/updates/2018/06/feature-policy
	https://scotthelme.co.uk/a-new-security-header-feature-policy/
	https://w3c.github.io/webappsec-feature-policy/
	https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Account/Login
Low (Medium)	No se encuentra encabezado X-Content-Type-Options Header
Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.
Solution	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web.
	Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Other Information	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Denuncias/Create
Parameter	X-Content-Type-Options
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/lib/bootstrap/dist/css/bootstrap.min.css
Low (Medium)	Feature Policy Header Not Set
(3110 011 01111)	r datary i dilay i daddi i tot det

Description	Feature Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Feature Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Feature-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy
	https://developers.google.com/web/updates/2018/06/feature-policy
	https://scotthelme.co.uk/a-new-security-header-feature-policy/
	https://w3c.github.io/webappsec-feature-policy/
	https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Account/Register
Low (Medium)	Feature Policy Header Not Set
Description	Feature Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Feature Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Feature-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy
	https://developers.google.com/web/updates/2018/06/feature-policy
	https://scotthelme.co.uk/a-new-security-header-feature-policy/
	https://w3c.github.io/webappsec-feature-policy/
	https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Account/Login
Low (Medium)	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma
Description	El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido.
Solution	Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache.
Reference	$https://www.owasp.org/index.php/Session_Management_Cheat_Sheet\#Web_Content_Caching$
CWE Id	525
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Denuncias/Create

Parameter	Cache-Control
Low (Medium)	No se encuentra encabezado X-Content-Type-Options Header
Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.
Solution	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por
	el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Other Information	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/img/DEnuncia_Ciudadana.jpg
Parameter	X-Content-Type-Options
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other
	frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	
Solution Reference	components may be subject to. Ensure that your web server, application server, load balancer, etc. is configured to suppress
	components may be subject to. Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-
	components may be subject to. Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
Reference CWE Id WASC Id	components may be subject to. Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html 200 13
Reference CWE Id WASC Id URL	components may be subject to. Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
Reference CWE Id WASC Id	components may be subject to. Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html 200 13
Reference CWE Id WASC Id URL	components may be subject to. Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html 200 13 https://vpsamvc.azurewebsites.net/img/Candado.png
Reference CWE Id WASC Id URL Low (Medium)	components may be subject to. Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html 200 13 https://vpsamvc.azurewebsites.net/img/Candado.png No se encuentra encabezado X-Content-Type-Options Header El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán

Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
16
15
https://vpsamvc.azurewebsites.net/lib/jquery/dist/jquery.min.js
X-Content-Type-Options
Incompleto o no Cache-control y sistema de encabezado HTTP Pragma
El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido.
Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache.
https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
525
13
https://vpsamvc.azurewebsites.net/Denuncias/View
https://vpsamvc.azurewebsites.net/Denuncias/View
https://vpsamvc.azurewebsites.net/Denuncias/View Cache-Control
Content Security Policy (CSP) Header Not Set Content Security Policy (CSP) Header Not Set 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,
Content Security Policy (CSP) Header Not Set Content Security Policy (CSP) Header Not Set 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. Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and
Content Security Policy (CSP) Header Not Set 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. Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+. https://developer.mozilla.org/en-
Content Security Policy (CSP) Header Not Set 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. Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+. https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
Content Security Policy (CSP) Header Not Set 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. Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+. https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html http://www.w3.org/TR/CSP/ http://www.w3.org/TR/CSP/ http://www.w3.cigithub.io/webappsec/specs/content-security-policy/csp-specification.dev.html
Cache-Control Content Security Policy (CSP) Header Not Set 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. Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+. https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html http://www.w3.org/TR/CSP/ http://www.html5rocks.com/en/tutorials/security/content-security-policy/
Content Security Policy (CSP) Header Not Set 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. Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+. https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html http://www.w3.org/TR/CSP/ http://www.w3.org/TR/CSP/ http://www.html5rocks.com/en/tutorials/security/content-security-policy/ http://caniuse.com/#feat=contentsecuritypolicy
Cache-Control Content Security Policy (CSP) Header Not Set 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. Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+. https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html http://www.w3.org/TR/CSP/ http://www.html5rocks.com/en/tutorials/security/content-security-policy/

WASC Id		15
URL		https://vpsamvc.azurewebsites.net/Account/Register
Low		, ,
	Server L	eaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	headers. A	pplication server is leaking information via one or more "X-Powered-By" HTTP response Access to such information may facilitate attackers identifying other frameworks/components application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that By" heade	at your web server, application server, load balancer, etc. is configured to suppress "X-Powered-rs.
Reference	http://blogs	s.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www	.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200	
WASC Id	13	
URL	https://vp:	samvc.azurewebsites.net/js/site.js?v=4q1jwFhaPaZgr8WAUSrux6hAuh0XDg9kPS3xlVq36
Low (Med	dium)	No se encuentra encabezado X-Content-Type-Options Header
Description		El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.
Solution		Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Other Inform	nation	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Reference		http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id		16
WASC Id		15
URL		https://vpsamvc.azurewebsites.net/denuncias/create
Parameter		X-Content-Type-Options
Low (Medium)	Feature	Policy Header Not Set
Description	usage of b specifying of standard	olicy Header is an added layer of security that helps to restrict from unauthorized access or prowser/client features by web resources. This policy ensures the user privacy by limiting or the features of the browsers can be used by the web resources. Feature Policy provides a set d HTTP headers that allow website owners to limit which features of browsers can be used by such as camera, microphone, location, full screen etc.
Solution		at your web server, application server, load balancer, etc. is configured to set the Feature-Policy

header.

Reference	https://dev	eloper.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy		
https://de		elopers.google.com/web/updates/2018/06/feature-policy		
	https://scot	ttps://scotthelme.co.uk/a-new-security-header-feature-policy/		
https://v		c.github.io/webappsec-feature-policy/		
		w.smashingmagazine.com/2018/12/feature-policy/		
CWE Id	16			
WASC Id	15			
URL	https://vpsamvc.azurewebsites.net/js/site.js?v=4q1jwFhaPaZgr8WAUSrux6hAuh0XDg9kPSI0			
Low (Med	dium)	Feature Policy Header Not Set		
Description		Feature Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Feature Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.		
Solution		Ensure that your web server, application server, load balancer, etc. is configured to set the Feature-Policy header.		
Reference		https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy		
		https://developers.google.com/web/updates/2018/06/feature-policy		
		https://scotthelme.co.uk/a-new-security-header-feature-policy/		
		https://w3c.github.io/webappsec-feature-policy/		
		https://www.smashingmagazine.com/2018/12/feature-policy/		
CWE Id		16		
WASC Id		15		
URL		https://vpsamvc.azurewebsites.net/lib/bootstrap/dist/js/bootstrap.bundle.min.js		
Low (Med	dium)	No se encuentra encabezado X-Content-Type-Options Header		
Description		El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.		
Solution		Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web.		
		Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.		
Other Inform	mation	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.		

Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Denuncias/View
Parameter	X-Content-Type-Options
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
CWE Id	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html 200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/lib/bootstrap/dist/js/bootstrap.bundle.min.js
Low (Medium)	
	No se encuentra encabezado X-Content-Type-Options Header
Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.
Solution	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por
Other Information	el servidor de la aplicación/web para no ejecutar MIME-sniffing. Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/css/site.css
Parameter	X-Content-Type-Options
Low (Medium)	No se encuentra encabezado X-Content-Type-Options Header
Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido

	declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.
Solution	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web.
	Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Other Information	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/img/Candado.png
Parameter	X-Content-Type-Options
Low (Medium)	Feature Policy Header Not Set
Description	Feature Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Feature Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Feature-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy
	https://developers.google.com/web/updates/2018/06/feature-policy
	https://scotthelme.co.uk/a-new-security-header-feature-policy/
	https://w3c.github.io/webappsec-feature-policy/
	https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Denuncias/View
Low (Medium)	Feature Policy Header Not Set
Description	Feature Policy Header is an added layer of security that helps to restrict from unauthorized
Description	access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Feature Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Feature-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

	https://developers.google.com/web/updates/2018/06/feature-policy
	https://scotthelme.co.uk/a-new-security-header-feature-policy/
	https://w3c.github.io/webappsec-feature-policy/
	https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/lib/jquery-validation- unobtrusive/jquery.validate.unobtrusive.min.js
Low (Medium)	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma
Description	El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido.
Solution	Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache.
Reference	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
CWE Id	525
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/lib/bootstrap/dist/css/bootstrap.min.css
Parameter	Cache-Control
Low (Medium)	Cookie sin bandera asegurada
D : /:	
Description	Una cookie ha sido enviada sin la bandera asegurada, lo que significa que la cookie puede ser accedida mediante conexiones sin cifrar.
Description Solution	
	accedida mediante conexiones sin cifrar. Cuando una cookie contiene información sensible o es un token de sesión, debería ser siempre pasada usando un canal cifrado. Asegúrese que la bandera asegurada está
Solution	accedida mediante conexiones sin cifrar. Cuando una cookie contiene información sensible o es un token de sesión, debería ser siempre pasada usando un canal cifrado. Asegúrese que la bandera asegurada está establecida para cookies conteniendo información sensible.
Solution Reference	accedida mediante conexiones sin cifrar. Cuando una cookie contiene información sensible o es un token de sesión, debería ser siempre pasada usando un canal cifrado. Asegúrese que la bandera asegurada está establecida para cookies conteniendo información sensible. http://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)
Solution Reference CWE Id	accedida mediante conexiones sin cifrar. Cuando una cookie contiene información sensible o es un token de sesión, debería ser siempre pasada usando un canal cifrado. Asegúrese que la bandera asegurada está establecida para cookies conteniendo información sensible. http://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002) 614
Solution Reference CWE Id WASC Id	accedida mediante conexiones sin cifrar. Cuando una cookie contiene información sensible o es un token de sesión, debería ser siempre pasada usando un canal cifrado. Asegúrese que la bandera asegurada está establecida para cookies conteniendo información sensible. http://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002) 614 13
Solution Reference CWE Id WASC Id URL	accedida mediante conexiones sin cifrar. Cuando una cookie contiene información sensible o es un token de sesión, debería ser siempre pasada usando un canal cifrado. Asegúrese que la bandera asegurada está establecida para cookies conteniendo información sensible. http://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002) 614 13 https://vpsamvc.azurewebsites.net/Account/Login
Solution Reference CWE Id WASC Id URL Parameter	accedida mediante conexiones sin cifrar. Cuando una cookie contiene información sensible o es un token de sesión, debería ser siempre pasada usando un canal cifrado. Asegúrese que la bandera asegurada está establecida para cookies conteniendo información sensible. http://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002) 614 13 https://vpsamvc.azurewebsites.net/Account/Login .AspNetCore.Antiforgery.w5W7x28NAIs
Solution Reference CWE Id WASC Id URL Parameter Low (Medium)	accedida mediante conexiones sin cifrar. Cuando una cookie contiene información sensible o es un token de sesión, debería ser siempre pasada usando un canal cifrado. Asegúrese que la bandera asegurada está establecida para cookies conteniendo información sensible. http://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002) 614 13 https://vpsamvc.azurewebsites.net/Account/Login .AspNetCore.Antiforgery.w5W7x28NAIs Absence of Anti-CSRF Tokens

*La victima tiene una sesión activa en el sitio de destino.

*La víctima se autoriza por medio de la autenticación HTTP en el sitio de destino.

*La víctima se encuentra en la misma red local que el sitio de destino.

CSRF se ha utilizado especialmente para poder realizar una acción contra un sitio objetivo utilizando los privilegios de la víctima, pero se han revelado técnicas recientes para difundir información al obtener el acceso a la respuesta. El riesgo de divulgación de información aumenta de forma drástica cuando el sitio de destino se encuentra vulnerable a XSS, porque XSS se puede utilizar como una plataforma para CSRF, lo que le permite al atacante que opere desde adentro de los líites de la misma política de origen.

Solution

Frase: Arquitectura y Diseño

Utilice una biblioteca o marco comprobado que no acepte que ocura esta debilidad o que proporcione construcciones que permitan que esta debilidad sea mas sencilla de evitar.

Por ejemplo, utilice el paquete anti-CSRG como el CSRGuard de OWASP.

Fase: Implementación

Asegúrese de que su aplicación esté libre de fallas de secuencias de comandos entre sitios, ya que la mayoría de las defensas de CSRF pueden detenerse por alto por medio del uso de secuencias de comandos manejadas por el atacante.

Fase: Arquitectura y Diseño

Origina un nonce único para cada uno de los formularios, coloque el nonce en el formularo y confirme la independencia al obtener el formulario. Asegúrese de que el nonce no sea predecible (CWE-330).

Usted tiene que tener en cuenta que esto puede pasar desapercibido utilizando XSS.

Identificar las operaciones que sean especialmente peligrosas. Cuando el usuario desarrolla una operación peligrosa, envíe una solicitud de confirmación de forma separada para poder garantizar que el usuario tenga la intención de desarrollar esa operación.

Usted tiene que tener en cuenta que esto puede pasar desapercibido utilizando XSS.

Utilice el control de gestión de la sesión de ESAPI.

Este control introduce un elemento para CSRF.

No utilice el método GET para ninguna de las solicitudes que puedan desencadenar un cambio de estado.

Fase: Implementación

Revise que la solicitud se creó en la página esperada. Esto podría quebrar la funcionalidad auténtica, ya que los usuarios o los representantes puede ser que hayan desactivado el envío de Referer por motivos de privacidad.

Other Information

No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret] was found in the following HTML form: [Form 2: "Denunciald"].

Reference	http://projects.webappsec.org/Cross-Site-Request-Forgery
	http://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
URL	https://vpsamvc.azurewebsites.net/Denuncias/View
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Denuncias/View
Low (Medium)	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma
Description	El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido.
Solution	Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache.
Reference	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
CWE Id	525
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Account
Parameter	Cache-Control
Low (Medium)	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma
Description	El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido.
Solution	Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache.
Reference	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
CWE Id	525
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/denuncias/create
Parameter	Cache-Control
Low (Medium)	Feature Policy Header Not Set
Description	Feature Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Feature Policy provides a set of standard HTTP headers that allow website owners

	to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Feature-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy
	https://developers.google.com/web/updates/2018/06/feature-policy
	https://scotthelme.co.uk/a-new-security-header-feature-policy/
	https://w3c.github.io/webappsec-feature-policy/
	https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Home
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/lib/jquery-validation- unobtrusive/jquery.validate.unobtrusive.min.js
Low (Medium)	Feature Policy Header Not Set
Description	Feature Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Feature Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Feature-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy
	https://developers.google.com/web/updates/2018/06/feature-policy
	https://scotthelme.co.uk/a-new-security-header-feature-policy/
	https://w3c.github.io/webappsec-feature-policy/
	https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id	16
WASC Id	15

URL	https://vpsamvc.azurewebsites.net/Account/Register
Low (Medium)	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma
Description	El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido.
Solution	Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache.
Reference	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
CWE Id	525
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Account/Register
Parameter	Cache-Control
Low (Medium)	Cookie sin bandera asegurada
Description	Una cookie ha sido enviada sin la bandera asegurada, lo que significa que la cookie puede ser accedida mediante conexiones sin cifrar.
Solution	Cuando una cookie contiene información sensible o es un token de sesión, debería ser siempre pasada usando un canal cifrado. Asegúrese que la bandera asegurada está establecida para cookies conteniendo información sensible.
Reference	http://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)
CWE Id	614
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/robots.txt
Parameter	ARRAffinity
Low (Medium)	Content Security Policy (CSP) Header Not Set
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.
Description Solution	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,
	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. Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and
Solution	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. Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+. https://developer.mozilla.org/en-
Solution	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. Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+. https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
Solution	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. Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+. https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
Solution	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. Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+. https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy_Cheat_Sheet.html https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
Solution	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. Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+. https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html http://www.w3.org/TR/CSP/
Solution	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. Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+. https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html http://www.w3.org/TR/CSP/ http://www.w3.org/TR/CSP/ http://www.html5rocks.com/en/tutorials/security/content-security-policy/

WASC Id		15
URL		https://vpsamvc.azurewebsites.net/denuncias/create
Low		Interior Pount on Law of the Section and Assistance Court
_	Server L	eaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	headers. A	pplication server is leaking information via one or more "X-Powered-By" HTTP response access to such information may facilitate attackers identifying other frameworks/components your ation is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that By" header	at your web server, application server, load balancer, etc. is configured to suppress "X-Powered-rs.
Reference	http://blogs	s.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www	.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200	
WASC Id	13	
URL	https://vps UserId	samvc.azurewebsites.net/Denuncias/View?Denunciald&Descripcion&EstadoDenunciald&
Low (Med	dium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description		The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution		Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference		http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
		http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id		200
WASC Id		13
URL		https://vpsamvc.azurewebsites.net/lib/fontawesome/webfonts/fa-solid-900.woff2
Low (Med	dium)	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma
Description		El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido.
Solution		Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache.
Reference		https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
CWE Id		525
WASC Id		13
URL		https://vpsamvc.azurewebsites.net/Account/Register
Parameter		Cache-Control
Low (Med	dium)	Content Security Policy (CSP) Header Not Set
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.
Solution		Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.
Reference		https://developer.mozilla.org/en- US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
		https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
		http://www.w3.org/TR/CSP/
		http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html
		http://www.html5rocks.com/en/tutorials/security/content-security-policy/
		http://caniuse.com/#feat=contentsecuritypolicy
		http://content-security-policy.com/
CWE Id		16
WASC Id		15
URL		https://vpsamvc.azurewebsites.net/Account/Login
Low		
(Medium	No se er	ncuentra encabezado X-Content-Type-Options Header
)		
Description	permite ve respuesta, tipo de cor antiguas de	zado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto risiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un trenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones e Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes ar el MIME-Sniffing.
Solution	_	que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web.
	Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.	
Other Information	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.	
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers	
CWE Id	16	
WASC Id	15	
URL	https://vps 10	samvc.azurewebsites.net/js/site.js?v=4q1jwFhaPaZgr8WAUSrux6hAuh0XDg9kPS3xIVq36
Parameter		-Type-Options
Low (Med	lium)	No se encuentra encabezado X-Content-Type-Options Header
Description		El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta

	sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.
Solution	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web.
	Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Other Information	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/img/VPSA.png
Parameter	X-Content-Type-Options
Low (Medium)	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma
Description	El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido.
Solution	Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache.
Reference CWE Id	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching 525
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Account/Login
Parameter	Cache-Control
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Denuncias/View
Low (Medium)	No se encuentra encabezado X-Content-Type-Options Header
Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido

	declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.
Solution	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web.
	Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Other Information	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Account/Register
Parameter	X-Content-Type-Options
L aver (Mandissee)	
Low (Medium)	Feature Policy Header Not Set
Description	Feature Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Feature Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Feature-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy
	https://developers.google.com/web/updates/2018/06/feature-policy
	https://scotthelme.co.uk/a-new-security-header-feature-policy/
	https://w3c.github.io/webappsec-feature-policy/
	https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/lib/jquery-validation/dist/jquery.validate.min.js
Low (Medium)	Cookie Without SameSite Attribute
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be
Description	sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	16
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Denuncias
Parameter	ARRAffinity

Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/robots.txt
Low (Medium)	No se encuentra encabezado X-Content-Type-Options Header
Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.
Solution	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Other Information	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/img/reclamos.jpg
Parameter	X-Content-Type-Options
Low (Medium)	Cookie sin bandera asegurada
Description	Una cookie ha sido enviada sin la bandera asegurada, lo que significa que la cookie puede ser accedida mediante conexiones sin cifrar.
Solution	Cuando una cookie contiene información sensible o es un token de sesión, debería ser siempre pasada usando un canal cifrado. Asegúrese que la bandera asegurada está establecida para cookies conteniendo información sensible.
Reference	http://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)
CWE Id	614
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Account/Register
Parameter	.AspNetCore.Antiforgery.w5W7x28NAIs

Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/img/DEnuncia_Ciudadana.jpg
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/lib/fontawesome/css/all.min.css
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header
Low (Mediani)	Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Home
Low (Medium)	No se encuentra encabezado X-Content-Type-Options Header
Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.

Solution	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándarse y moderne que no ciacuta MIME eniffina en absoluta e que puede par dirigido par
	estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Other Information	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Account/Register
Parameter	X-Content-Type-Options
Low (Medium)	Content Security Policy (CSP) Header Not Set
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.
Reference	https://developer.mozilla.org/en- US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
	https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
	http://www.w3.org/TR/CSP/
	http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html
	http://www.html5rocks.com/en/tutorials/security/content-security-policy/
	http://caniuse.com/#feat=contentsecuritypolicy
	http://content-security-policy.com/
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Account
Low (Medium)	Feature Policy Header Not Set
Description	Feature Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Feature Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.

0.1.4	
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Feature-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy
	https://developers.google.com/web/updates/2018/06/feature-policy
	https://scotthelme.co.uk/a-new-security-header-feature-policy/
	https://w3c.github.io/webappsec-feature-policy/
	https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/lib/toastr/toastr.min.js
Low (Medium)	No se encuentra encabezado X-Content-Type-Options Header
Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.
Solution	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Other Information	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/img/Obras.jpg
Parameter	X-Content-Type-Options
Low (Medium)	Cookie Without SameSite Attribute
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	16
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Account
Parameter	ARRAffinity
Low (Medium)	No se encuentra encabezado X-Content-Type-Options Header

Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.
Solution	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los
	estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Other Information	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Denuncias
Parameter	X-Content-Type-Options
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header
	Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/lib/jquery/dist/jquery.min.js
Low (Medium)	Feature Policy Header Not Set
Description	Feature Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Feature Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Feature-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy
	https://developers.google.com/web/updates/2018/06/feature-policy
	https://scotthelme.co.uk/a-new-security-header-feature-policy/

	https://w2c.github.io/wohonness.footure.noligy/
	https://w3c.github.io/webappsec-feature-policy/
	https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/lib/Datatables/datatables.min.js
Low (Medium)	Content Security Policy (CSP) Header Not Set
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.
Reference	https://developer.mozilla.org/en- US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
	https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
	http://www.w3.org/TR/CSP/
	http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html
	http://www.html5rocks.com/en/tutorials/security/content-security-policy/
	http://caniuse.com/#feat=contentsecuritypolicy
	http://content-security-policy.com/
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Denuncias/View
Low (Medium)	Content Security Policy (CSP) Header Not Set
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.
Reference	https://developer.mozilla.org/en- US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
	https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html

	http://www.w3.org/TR/CSP/
	http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html
	http://www.html5rocks.com/en/tutorials/security/content-security-policy/
	http://caniuse.com/#feat=contentsecuritypolicy
	http://content-security-policy.com/
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Denuncias
Low (Medium)	No se encuentra encabezado X-Content-Type-Options Header
Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.
Solution	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web.
	Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Other Information	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Home
Parameter	X-Content-Type-Options
Low (Medium)	No se encuentra encabezado X-Content-Type-Options Header
Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.
Solution	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web.
	Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Other Information	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay

	preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/lib/jquery-validation/dist/jquery.validate.min.js
Parameter	X-Content-Type-Options
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/lib/Datatables/datatables.min.css
Low (Medium)	No se encuentra encabezado X-Content-Type-Options Header
Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para
	'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME- sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.
Solution	sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por
Solution Other Information	sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web.
	sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing. Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En
Other Information	sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing. Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor. http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx
Other Information Reference	sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing. Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor. http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
Other Information Reference CWE Id	sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing. Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor. http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
Other Information Reference CWE Id WASC Id	sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing. Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor. http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers 16
Other Information Reference CWE Id WASC Id URL	sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing. Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor. http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers 16 15 https://vpsamvc.azurewebsites.net/Account

	sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.
Solution	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web.
	Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Other Information	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/lib/Datatables/datatables.min.js
Parameter	X-Content-Type-Options
Low (Medium)	No se encuentra encabezado X-Content-Type-Options Header
Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.
Solution	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Other Information	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/favicon.ico
Parameter	X-Content-Type-Options
Low (Medium)	Cookie sin bandera asegurada
Description	Una cookie ha sido enviada sin la bandera asegurada, lo que significa que la cookie puede ser accedida mediante conexiones sin cifrar.
Solution	Cuando una cookie contiene información sensible o es un token de sesión, debería ser siempre pasada usando un canal cifrado. Asegúrese que la bandera asegurada está establecida para cookies conteniendo información sensible.
Reference	http://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)
CWE Id	614

URL Parameter	https://vpsamvc.azurewebsites.net/Denuncias
Parameter	A D.D. Affinity
	ARRAffinity
Low (Medium)	Cookie sin bandera asegurada
Description	Una cookie ha sido enviada sin la bandera asegurada, lo que significa que la cookie puede ser accedida mediante conexiones sin cifrar.
Solution	Cuando una cookie contiene información sensible o es un token de sesión, debería ser siempre pasada usando un canal cifrado. Asegúrese que la bandera asegurada está establecida para cookies conteniendo información sensible.
Reference	http://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)
CWE Id	614
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Account
Parameter	.AspNetCore.Antiforgery.w5W7x28NAIs
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
CWE Id	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
WASC Id	200 13
URL	https://vpsamvc.azurewebsites.net/img/reclamos.jpg
Low (Medium)	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma
	El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido.
	Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache.
Reference	$https://www.owasp.org/index.php/Session_Management_Cheat_Sheet \#Web_Content_Caching$
	525
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/css/site.css
Parameter	Cache-Control
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.

Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/lib/toastr/toastr.min.css
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Account/Register
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Denuncias/Create
Low (Medium)	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma
Description	El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido.
Solution	Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache.
Reference	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
CWE Id	525
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/lib/Datatables/datatables.min.css
Parameter	Cache-Control
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Account/Register
Low (Medium)	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma
, ,	· · · ·
Description	El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido.
Solution	Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache.
Reference	$https://www.owasp.org/index.php/Session_Management_Cheat_Sheet \#Web_Content_Caching$
CWE Id	525
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Denuncias
Parameter	Cache-Control
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-
	headers.aspx
OMETH	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
WASC Id	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html 200
WASC Id URL	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html 200 13 https://vpsamvc.azurewebsites.net/favicon.ico
WASC Id	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html 200
WASC Id URL	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html 200 13 https://vpsamvc.azurewebsites.net/favicon.ico
WASC Id URL Low (Medium)	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html 200 13 https://vpsamvc.azurewebsites.net/favicon.ico No se encuentra encabezado X-Content-Type-Options Header El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán

	Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Other Information	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/lib/fontawesome/webfonts/fa-solid-900.woff2
Parameter	X-Content-Type-Options
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
WASC Id URL	13 https://vpsamvc.azurewebsites.net/Denuncias/Create
URL	https://vpsamvc.azurewebsites.net/Denuncias/Create
URL <mark>Low (Medium)</mark>	No se encuentra encabezado X-Content-Type-Options Header El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán
URL Low (Medium) Description	No se encuentra encabezado X-Content-Type-Options Header El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff'
URL Low (Medium) Description	No se encuentra encabezado X-Content-Type-Options Header El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por
URL Low (Medium) Description Solution	No se encuentra encabezado X-Content-Type-Options Header El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing. Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En
URL Low (Medium) Description Solution Other Information	No se encuentra encabezado X-Content-Type-Options Header El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing. Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor. http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
URL Low (Medium) Description Solution Other Information Reference CWE Id WASC Id	No se encuentra encabezado X-Content-Type-Options Header El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing. Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor. http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers 16
URL Low (Medium) Description Solution Other Information Reference CWE Id WASC Id URL	No se encuentra encabezado X-Content-Type-Options Header El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing. Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor. http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers 16 15 https://vpsamvc.azurewebsites.net/lib/Datatables/datatables.min.css
URL Low (Medium) Description Solution Other Information Reference CWE Id WASC Id	No se encuentra encabezado X-Content-Type-Options Header El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing. Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor. http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers 16

Low (Medium)	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma
Description	El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido.
Solution	Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache.
Reference	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
CWE Id	525
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Home
Parameter	Cache-Control
Low (Medium)	No se encuentra encabezado X-Content-Type-Options Header
Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.
Solution	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web.
	Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Other Information	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/lib/bootstrap/dist/css/bootstrap.min.css
Parameter	X-Content-Type-Options
Low (Medium)	No se encuentra encabezado X-Content-Type-Options Header
Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.
Solution	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web.
	Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Other Information	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay

	preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/lib/bootstrap/dist/js/bootstrap.bundle.min.js
Parameter	X-Content-Type-Options
Low (Medium)	Cookie sin bandera asegurada
Description	Una cookie ha sido enviada sin la bandera asegurada, lo que significa que la cookie puede ser accedida mediante conexiones sin cifrar.
Solution	Cuando una cookie contiene información sensible o es un token de sesión, debería ser siempre pasada usando un canal cifrado. Asegúrese que la bandera asegurada está establecida para cookies conteniendo información sensible.
Reference	http://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)
CWE Id	614
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Account
Parameter	ARRAffinity
Low (Medium)	Feature Policy Header Not Set
Description	Feature Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Feature Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Feature-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy https://developers.google.com/web/updates/2018/06/feature-policy https://scotthelme.co.uk/a-new-security-header-feature-policy/ https://w3c.github.io/webappsec-feature-policy/ https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Denuncias/Create
Low (Medium)	Feature Policy Header Not Set
Description	Feature Policy Header Not Set Feature Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Feature Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Feature-Policy header.

Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy
	https://developers.google.com/web/updates/2018/06/feature-policy
	https://scotthelme.co.uk/a-new-security-header-feature-policy/
	https://w3c.github.io/webappsec-feature-policy/
	https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Account
Low (Medium)	Cookie sin bandera asegurada
Description	Una cookie ha sido enviada sin la bandera asegurada, lo que significa que la cookie puede ser
Безсприон	accedida mediante conexiones sin cifrar.
Solution	Cuando una cookie contiene información sensible o es un token de sesión, debería ser siempre pasada usando un canal cifrado. Asegúrese que la bandera asegurada está establecida para cookies conteniendo información sensible.
Reference	http://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)
CWE Id	614
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Account/Register
Parameter	ARRAffinity
Low (Medium)	Cookie sin bandera asegurada
Description	Una cookie ha sido enviada sin la bandera asegurada, lo que significa que la cookie puede ser accedida mediante conexiones sin cifrar.
Solution	Cuando una cookie contiene información sensible o es un token de sesión, debería ser siempre pasada usando un canal cifrado. Asegúrese que la bandera asegurada está establecida para cookies conteniendo información sensible.
Reference	http://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)
CWE Id	614
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Denuncias
Parameter	.AspNetCore.Antiforgery.w5W7x28NAIs
Low (Medium)	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma
Description	El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido.
Solution	Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache.
Reference	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
CWE Id	525
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Denuncias/Create
Parameter	Cache-Control
Low (Medium)	Cookie Without SameSite Attribute

Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	16
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/robots.txt
Parameter	ARRAffinity
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/css/site.css
Low (Madium)	No an analysis and a second by Constant Town Cottons Has been
Low (Medium)	No se encuentra encabezado X-Content-Type-Options Header
Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán
	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido
Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff'
Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por
Description Solution	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing. Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En
Description Solution Other Information	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing. Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor. http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx
Description Solution Other Information Reference CWE Id WASC Id	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing. Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor. http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
Description Solution Other Information Reference CWE Id	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing. Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor. http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
Description Solution Other Information Reference CWE Id WASC Id	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing. Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor. http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers 16 15 https://vpsamvc.azurewebsites.net/lib/jquery-validation-

Description	actions Delice Handon in an added in the first of the fir
ac pr re to	eature Policy Header is an added layer of security that helps to restrict from unauthorized ccess or usage of browser/client features by web resources. This policy ensures the user rivacy by limiting or specifying the features of the browsers can be used by the web esources. Feature Policy provides a set of standard HTTP headers that allow website owners or limit which features of browsers can be used by the page such as camera, microphone, ecation, full screen etc.
Solution En	nsure that your web server, application server, load balancer, etc. is configured to set the eature-Policy header.
Reference ht	ttps://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy
ht	ttps://developers.google.com/web/updates/2018/06/feature-policy
ht	ttps://scotthelme.co.uk/a-new-security-header-feature-policy/
ht	ttps://w3c.github.io/webappsec-feature-policy/
ht	ttps://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id 16	6
WASC Id 15	5
URL ht	ttps://vpsamvc.azurewebsites.net/Denuncias/Create
	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
re fra	he web/application server is leaking information via one or more "X-Powered-By" HTTP esponse headers. Access to such information may facilitate attackers identifying other ameworks/components your web application is reliant upon and the vulnerabilities such omponents may be subject to.
	nsure that your web server, application server, load balancer, etc. is configured to suppress K-Powered-By" headers.
he	ttp://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-eaders.aspx
	ttp://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
	00 3
WASC Id 13	
	ttps://vpsamvc.azurewebsites.net/Denuncias
,	Server Leaks Information via "X-Powered-By" HTTP Response Header
	ield(s)
re fra	he web/application server is leaking information via one or more "X-Powered-By" HTTP esponse headers. Access to such information may facilitate attackers identifying other ameworks/components your web application is reliant upon and the vulnerabilities such omponents may be subject to.
	nsure that your web server, application server, load balancer, etc. is configured to suppress K-Powered-By" headers.
he	ttp://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-eaders.aspx
	ttp://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
	00
WASC Id	
	ttps://vpsamvc.azurewebsites.net/Account/Login
	Server Leaks Information via "X-Powered-By" HTTP Response Header ield(s)

Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/img/Obras.jpg
Low (Medium)	Feature Policy Header Not Set
Description	Feature Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Feature Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Feature-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy
	https://developers.google.com/web/updates/2018/06/feature-policy
	https://scotthelme.co.uk/a-new-security-header-feature-policy/
	https://w3c.github.io/webappsec-feature-policy/
	https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Denuncias
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Account/Login
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
	http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/denuncias/create
Low (Medium)	No se encuentra encabezado X-Content-Type-Options Header
Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.
Solution	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los
	estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Other Information	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/Denuncias/Create
Parameter	X-Content-Type-Options
Low (Medium)	No se encuentra encabezado X-Content-Type-Options Header
Description	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.
Solution	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web.
	Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.
Other Information	Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay

	preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
Reference	http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
URL	https://vpsamvc.azurewebsites.net/lib/toastr/toastr.min.js
Parameter	X-Content-Type-Options
Low (Medium)	Feature Policy Header Not Set
Description	Feature Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Feature Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Feature-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy
	https://developers.google.com/web/updates/2018/06/feature-policy
	https://scotthelme.co.uk/a-new-security-header-feature-policy/
	https://w3c.github.io/webappsec-feature-policy/
	https://www.smashingmagazine.com/2018/12/feature-policy/
CWE ld	https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id WASC Id	
	16
WASC Id	16 15
WASC Id URL	16 15 https://vpsamvc.azurewebsites.net/denuncias/create
WASC Id URL Low (Medium)	15 https://vpsamvc.azurewebsites.net/denuncias/create No se encuentra encabezado X-Content-Type-Options Header El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán
WASC Id URL Low (Medium) Description	https://vpsamvc.azurewebsites.net/denuncias/create No se encuentra encabezado X-Content-Type-Options Header El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff'
WASC Id URL Low (Medium) Description Solution Other Information	https://vpsamvc.azurewebsites.net/denuncias/create No se encuentra encabezado X-Content-Type-Options Header El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing. Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.
WASC Id URL Low (Medium) Description Solution	https://vpsamvc.azurewebsites.net/denuncias/create No se encuentra encabezado X-Content-Type-Options Header El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing. Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En
WASC Id URL Low (Medium) Description Solution Other Information Reference CWE Id	https://vpsamvc.azurewebsites.net/denuncias/create No se encuentra encabezado X-Content-Type-Options Header El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing. Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor. http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
WASC Id URL Low (Medium) Description Solution Other Information Reference	https://vpsamvc.azurewebsites.net/denuncias/create No se encuentra encabezado X-Content-Type-Options Header El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web complatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing. Este inconveniente aún aplica para páginas de error (401, 403, 500, etc) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor. http://msdn.Microsoft.com/en-us/library/le/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers

Parameter	X-Content-Type-Options
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/sitemap.xml
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
URL	https://vpsamvc.azurewebsites.net/Account
Low (Medium)	Content Security Policy (CSP) Header Not Set
, ,	
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.
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.
Reference	https://developer.mozilla.org/en- US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
	https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
	http://www.w3.org/TR/CSP/
	http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html

		http://www.html5rocks.com/en/tutorials/security/content-security-policy/		
		http://caniuse.com/#feat=contentsecuritypolicy		
		http://content-security-policy.com/		
CWE Id		16		
WASC Id		15		
URL		https://vpsamvc.azurewebsites.net/Home		
Low (Lo	w)	Dangerous JS Functions		
Description	า	A dangerous JS function seems to be in use that would leave the site vulnerable.		
Solution		See the references for security advice on the use of these functions.		
Reference		https://angular.io/guide/security		
CWE Id		749		
URL		https://vpsamvc.azurewebsites.net/lib/jquery-validation- unobtrusive/jquery.validate.unobtrusive.min.js		
Low (Lo	w)	Dangerous JS Functions		
Description	ו	A dangerous JS function seems to be in use that would leave the site vulnerable.		
Solution		See the references for security advice on the use of these functions.		
Reference		https://angular.io/guide/security		
CWE Id		749		
URL		https://vpsamvc.azurewebsites.net/lib/bootstrap/dist/js/bootstrap.bundle.min.js		
Low (Lo	w)	Dangerous JS Functions		
Description	า	A dangerous JS function seems to be in use that would leave the site vulnerable.		
Solution		See the references for security advice on the use of these functions.		
Reference		https://angular.io/guide/security		
CWE Id		749		
URL		https://vpsamvc.azurewebsites.net/lib/jquery/dist/jquery.min.js		
Reference				
CWE Id	200			
WASC Id	13			
URL	https://vpsa	amvc.azurewebsites.net/lib/jquery/dist/jquery.min.js		