Revista Nexos Científicos *ISSN: 2773-7489*
Enero – Junio 2021 pp. 1-8 *Correo: editor@istvidanueva.edu.ec*
Volumen 5, Número 1 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: febrero 2021 *Fecha de aceptación: marzo 2021*

Aplicación de Vega Vulnerability Scanner en Aplicaciones Web

Aguas Luis [1]; Wladimir Paredes[2]

[1] *Universidad Tecnológica Israel-Departamento de Ciencias de la Ingeniería –Carrera de Sistemas, Quito, Ecuador, aguaszoft@Live.com;*
[2]*Instituto Superior Universitario Rumiñahui, Dirección de Investigación, Quito, Ecuador, wladimir.paredes@ister.edu.ec*

Resumen: En primer lugar, Vega es un escáner de seguridad web gratuito y de código ab-ierto que permite realizar pruebas de seguridad a aplicaciones web. Dentro de las pruebas de seguridad se pueden encontrar vulnerabilidades como Inyección SQL, Cross-Site Scripting (XSS), información confidencial revelada inadvertidamente entre otras vulnerabilidades (Murashka, 2020). Tras la breve introducción, esta herramienta va a permitir encontrar distintas vulnerabilidades e identificar las posibles mejoras a realizar. Esta herramienta se la va aplicar en 3 sitios web conocidos y encontrar sus vulnerabilidades.

Palabras clave: Inyección SQL, Cross-Site Scripting, Aplicación Web.

Vega Vulnerability Scanner Application in Web Applications

Abstract: First, Vega is a free and open source web security scanner that allows security testing of web applications. Vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), confidential information inadvertently revealed among other vulnerabilities can be found within security tests. Vulnerabilities such as SQL In-jection, Cross-Site Scripting (XSS), confidential information inadvertently re-vealed among other vulnerabilities can be found within security tests. This tool will be applied on 3 known websites and will find its vulnerabilities.

Keywords: SQL Injection, Cross-Site Scripting, Web Applications.

1. INTRODUCCIÓN

Decidimos trabajar en dos ambientes distintos Windows y OS X. El ambiente OS X para realizar la demostración de la metodología y el ambiente Windows para realizar generar los resultados. Lo primero fue descargar de la página oficial la herramienta Vega los archivos .exe y .dmg respectivamente.

Fig. 1. Archivos de instalación.

Entonces en cada equipo se procede a realizar la instalación de la herramienta Vega Scanner. Adicional se valida durante este proceso cualquier software que pueda necesitar la herramienta.

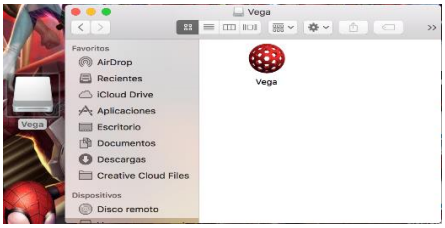

Fig. 2. Archivo .dmg instalación en OS X.

Fig. 3. Archivo .exe instalación en Windows.

1. Magíster en Redes de Comunicaciones, aguaszoft@Live.com
2. Tecnólogo en Análisis de Sistemas, henry.red1@hotmail.com
3. Tecnólogo en Gestión Informática, sammysislema94@hotmail.com

Revista Nexos Científicos *ISSN: 2773-7489*
Enero – Junio 2021 pp. 1-8 *Correo: editor@istvidanueva.edu.ec*
Volumen 5, Número 1 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: febrero 2021 *Fecha de aceptación: marzo 2021*

Nota: Dentro del proceso de instalación en ambos ambientes se pudo necesitar instalar el JRE2 o similar. Siendo que el proceso de instalación no es el objetivo primario de este trabajo no se lo va describir paso a paso.

Con los procesos de instalación completos, se tiene la herramienta lista para utilizarse y realizar el análisis.

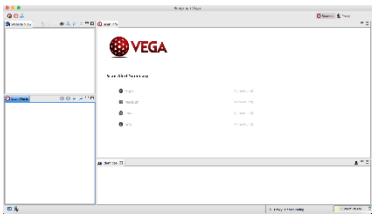

Fig. 4. Ventana de VEGA en OS X.

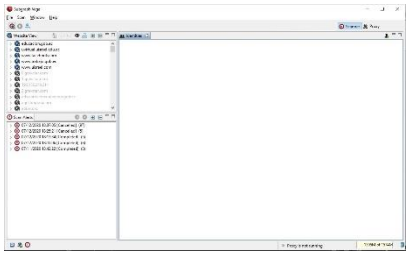

Fig. 5. Ventana de VEGA en Windows.

Para este análisis se escogieron 3 páginas de 2 entidades de Ecuador y 1 página de uso cotidiano. Detalladas a continuación:

Páginas	Dirección
Ministerio de Educación	https://educacion.gob.ec/
Facebook	https://www.facebook.com/
Ministerio de Trabajo	http://www.trabajo.gob.ec/

Para este trabajo lo que se busca es realizar un análisis de estas 3 páginas escogidas y encontrar sus posibles vulnerabilidades y de encontrarse alguna presentar las posibles soluciones que ofrece la herramienta Vega.

2. METODOLOGÍA

Una vez instalada la herramienta se va a utilizar una prueba de seguridad estándar, es decir con los valores por defecto que se nos presenten. A continuación se va a describir el proceso a realizarse con las páginas escogidas y cuales elementos son los que serán considerados para el análisis.

Nota: Se tomó como ejemplo el siguiente sitio web http://www.hotelresidencial.com.mx/ para mostrar los elementos a considerar para el análisis en el ambiente de OSX.

Se ejecuta el programa Vega dentro de las aplicaciones instaladas. Y a continuación se va a dar clic sobre el ícono  para empezar un nuevo análisis y se desplegará la siguiente ventana.

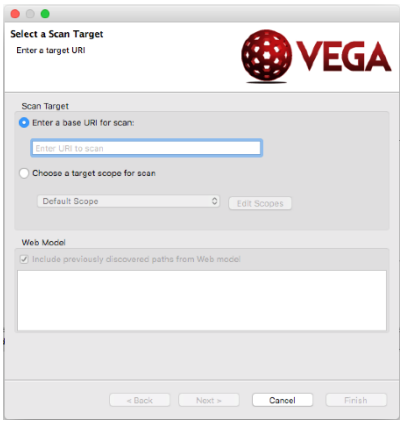

Fig. 6. Ventana de VEGA.

En esta ventana se ingresa la ip o la URI correspondiente a la que se va a realizar la prueba. Para este caso se va ingresar la url http://www.hotelresidencial.com.mx/ y se da clic en Next.

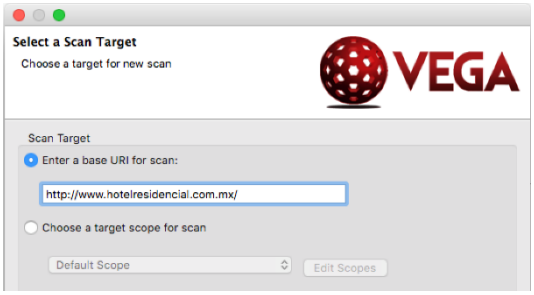

Fig. 7. Ventana de VEGA URI objetivo.

Después de ingresar la url aparece la siguiente ventana donde se seleccionan los diferentes

[2] JRE. Acrónimo de Java Runtime Enviroment. Conjunto de herramientas que permiten ejecutar código compilado en para el lenguaje de programación Java. [7]

Revista Nexos Científicos *ISSN: 2773-7489*
Enero – Junio 2021 pp. 1-8 *Correo: editor@istvidanueva.edu.ec*
Volumen 5, Número 1 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: febrero 2021 *Fecha de aceptación: marzo 2021*

Módulos de Escaneo para realizar las pruebas de seguridad.
Los módulos son unidades de funcionalidad extendida escritas en Javascript (Vega-Scanner, 2020).

Para esta prueba escogeremos los módulos de defecto seleccionados por la herramienta. Y se da clic en Next.

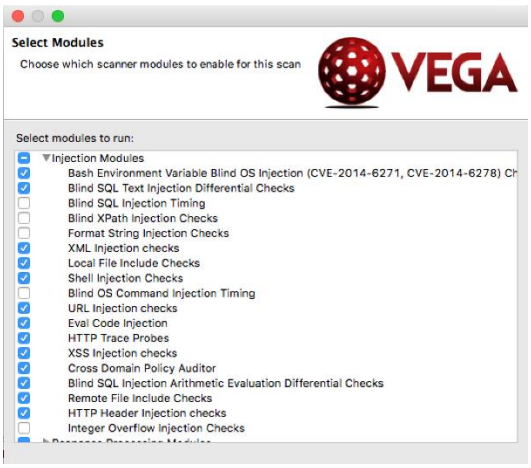

Fig. 8. Ventana de VEGA Módulos.

En la siguiente ventana se puede configurar alguna Cookie con la que se desee trabajar dentro de la aplicación Web. Pero para esta prueba no se incluirá ninguna y se dará clic en Next para continuar.

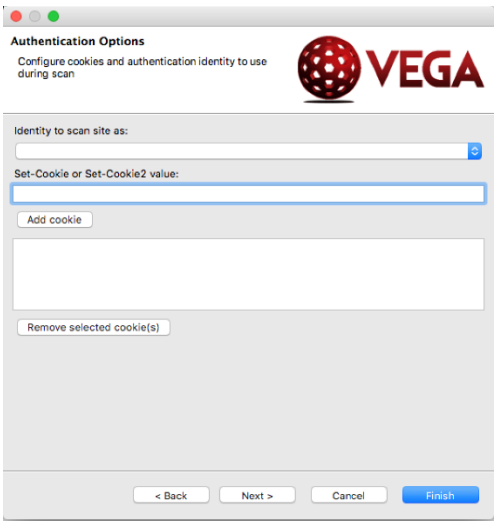

Fig. 9. Ventana de VEGA Opciones de Autenticación.

Y finalmente se muestra la siguiente ventana, donde se muestra una lista de parámetros que se van a excluir dentro del escaneo. Para esta prueba se va a utilizar los parámetros por defecto. Y se da clic en Finish.

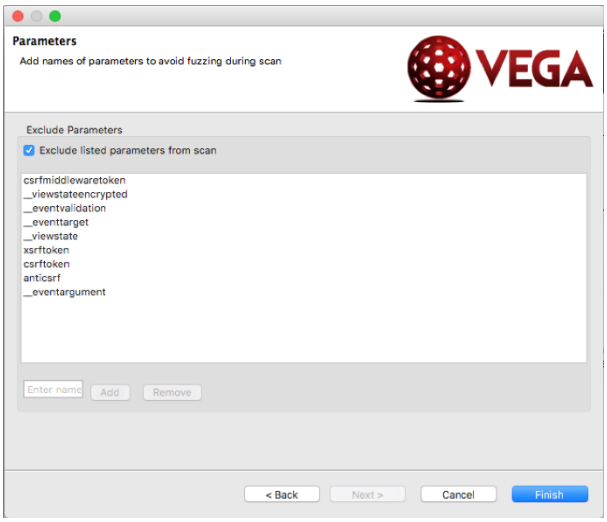

Fig. 10. Ventana de VEGA Parámetros.

En este momento, la herramienta comienza a trabajar sobre dicho sitio. Y comienza a realizar cada uno de los módulos definidos.

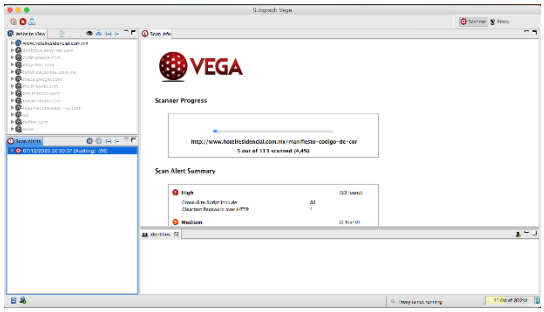

Fig. 11. Ventana de VEGA inicio escaneo.

En la pantalla principal hay dos elementos importantes el proceso de escaneo (Scanner Process) y el resumen de alertas de escaneo (Scan Alert Summary).

El proceso de escaneo muestra el avance del escaneo y las pruebas que faltan por realizar a todo el sitio junto a un porcentaje.

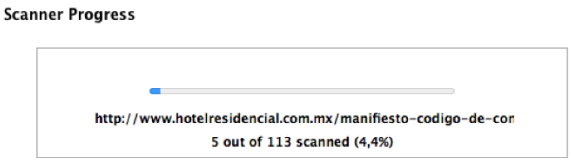

Fig. 12. Ventana de VEGA inicio escaneo.

Nota: Este proceso puede tardar un tiempo dependiendo del tamaño de la aplicación web a analizar.

Revista Nexos Científicos
Enero – Junio 2021 pp. 1-8
Volumen 5, Número 1
Fecha de recepción: febrero 2021
ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: marzo 2021

El resumen de alertas de escaneo muestra de forma clasificada las diferentes y un número que identifica cuantas incidencias del mismo tipo ha encontrado.

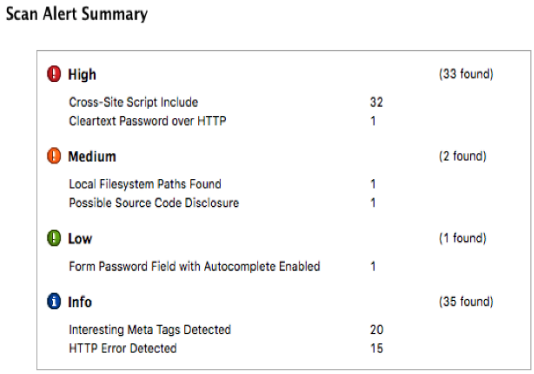

Fig. 13. Ventana de VEGA Resumen de Alertas.

Una vez completado el escaneo en la parte de alertas de escaneo (Scan Alerts) se puede visualizar todas las vulnerabilidades encontradas. Si se escoge una de las vulnerabilidades, para esta demostración se escogió Cleartext Password over HTTP.

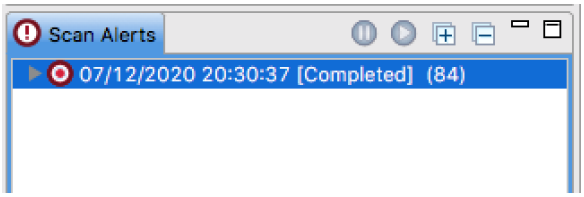

Fig. 14. Ventana de VEGA Alerta de escaneo.

En la ventana principal se desplegará información sobre la vulnerabilidad encontrada como, en que página encontró dicha vulnerabilidad, en que parte del código puede encontrarse, el impacto que puede tener y cuál es la recomendación que se debería realizar para solventar dicha vulnerabilidad.

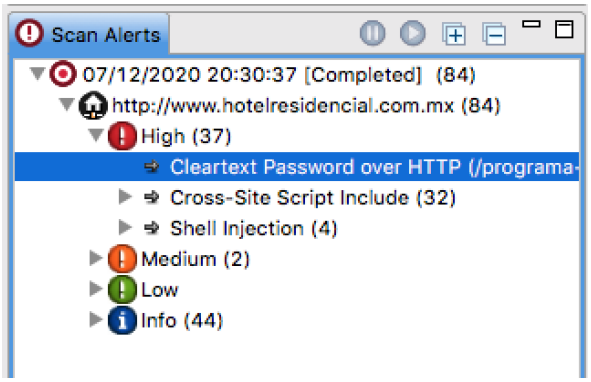

Fig. 15. Ventana de VEGA Detalle de alerta de escaneo.

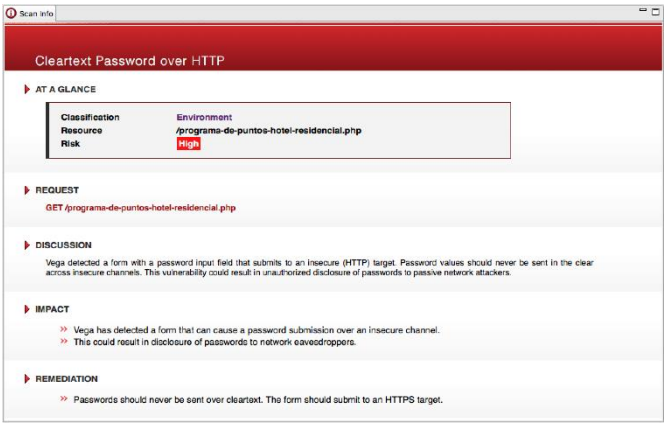

Fig. 16. Ventana de VEGA Información de escaneo.

3. RESULTADOS Y DISCUSIÓN

a. Primera prueba en Windows en primera página.

La primera prueba se realizó utilizando la url https://educacion.gob.ec/ que pertenece al Ministerio de Educación.

Se utilizaron los valores por defecto en la herramienta para el análisis de esta página obteniendo los siguientes resultados.

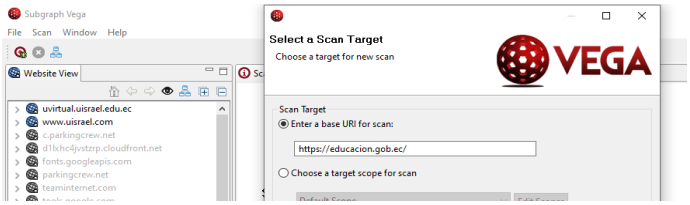

Fig. 17. Ventana de VEGA ingreso de primera url.

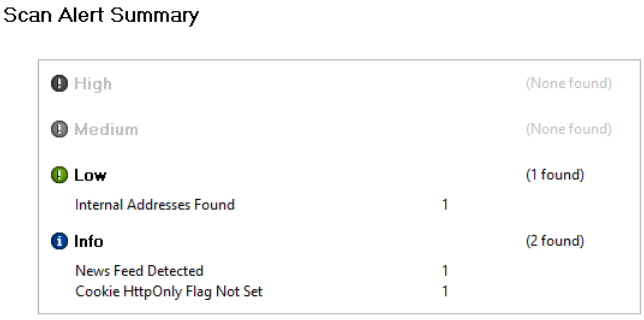

Fig. 18. Ventana de VEGA resultado de primer url.

Como se puede ver en las ilustraciones no se encontró ninguna vulnerabilidad de nivel Alto o Medio, que pueda ser susceptible a un ataque. Pero encontró una vulnerabilidad de nivel Bajo, lo cual detalla lo siguiente.

Revista Nexos Científicos
Enero – Junio 2021 pp. 1-8
Volumen 5, Número 1
Fecha de recepción: febrero 2021
ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: marzo 2021

Classification	Information
Resource	/
Risk	Low

Fig. 19. Riesgos

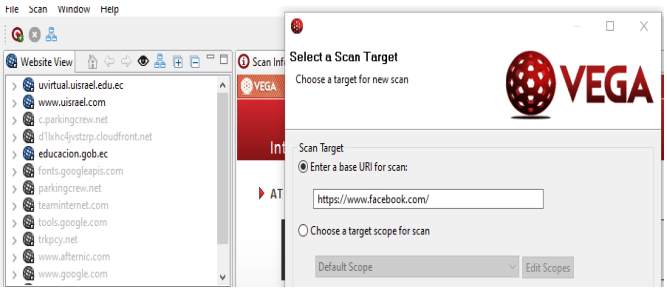

Fig. 20. Ventana de VEGA ingreso de segunda url.

Discusión

Vega ha descubierto referencias a hosts internos o redes en contenido de acceso público. Estas direcciones pueden revelar información a un atacante sobre la estructura interna de la red, lo que aumenta la probabilidad de éxito para ataques ciegos que involucran otras vulnerabilidades.

Impacto

Puede revelar la estructura de la red interna a atacantes externos.
Las direcciones IP internas que se han revelado podrían usarse como objetivos en ataques ciegos.

Remediación

La causa puede estar relacionada con el código, el contenido o debido a la configuración del entorno del servidor.

Se recomienda inspeccionar la página descubierta para determinar dónde se origina la dirección expuesta.

b. Segunda prueba en Windows en segunda página.

En la segunda prueba se utilizó la url https://www.facebook.com/ que pertenece a la red social Facebook.

Se utilizaron los valores por defecto en la herramienta para el análisis de esta página obteniendo los siguientes resultados.

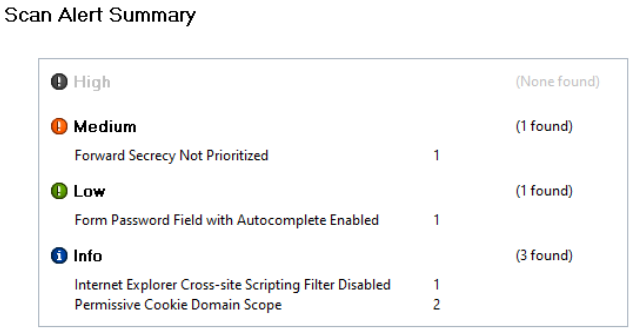

Fig. 21. Ventana de VEGA resultado de segunda url.

Como se puede ver en las ilustraciones se encontró una vulnerabilidad de nivel Medio que más adelante se detalla su tratamiento. Aunque se tengan otras vulnerabilidades de nivel Bajo, no se va tomar en cuenta para esta prueba.

Classification	Configuration
Risk	Medium

Fig. 22. Riesgo Medio

Discusión

Vega detectó que el servidor no prioriza los cifrados secretos hacia adelante en la lista de conjuntos de cifrado admitidos. Los cifrados secretos hacia adelante utilizan algoritmos como Diffie-Hellman efímero para generar una clave de sesión de un solo uso. Esta clave no se deriva de la clave privada a largo plazo, por lo tanto, la seguridad de los datos no está sujeta a descifrado si esa clave se ve comprometida en el futuro.

Impacto

Si no se utiliza un cifrado secreto directo, la seguridad de los datos de la sesión es tan segura como la clave privada a largo plazo del servidor.

Revista Nexos Científicos *ISSN: 2773-7489*
Enero – Junio 2021 pp. 1-8 *Correo: editor@istvidanueva.edu.ec*
Volumen 5, Número 1 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: febrero 2021 *Fecha de aceptación: marzo 2021*

Remediación

Los administradores del servidor deben configurar el servidor para priorizar los conjuntos de cifrado de reenvío secreto, como los que utilizan ECDHE (curva elíptica DH efímera) y DHE (DH efímera).
Mozilla ha puesto a disposición guías para configurar de forma segura los servidores TLS[3].
Es probable que se deba reiniciar el servidor HTTPS para que los cambios de configuración surtan efecto.

c. Tercera prueba en Windows en tercera página

En la última página se realizó utilizando la url http://www.trabajo.gob.ec/ que pertenece al Ministerio de Trabajo.

Se utilizaron los valores por defecto en la herramienta para el análisis de esta página obteniendo los siguientes resultados.

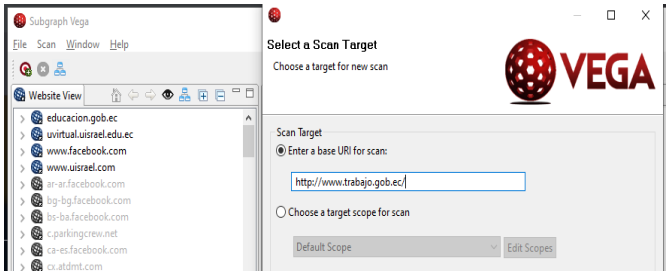

Fig. 23. Ventana de VEGA ingreso de tercera url.

Scan Alert Summary

High		(1 found)
Cleartext Password over HTTP	1	
Medium		(1 found)
HTTP Trace Support Detected	1	
Low		(1 found)
Form Password Field with Autocomplete Enabled	1	
Info		(94 found)
News Feed Detected	1	
Blank Body Detected	11	
HTTP Error Detected	68	
Character Set Not Specified	1	
Cookie HttpOnly Flag Not Set	12	
Interesting Meta Tags Detected	1	

Fig. 24. Ventana de VEGA resultado de tercera url.

Como se puede ver en las ilustraciones se encontró una vulnerabilidad de Nivel Alto y de Nivel medio que se va a detallar a continuación junto a su recomendación para corregirlo.

Classification	Environment
Resource	**/wp-login.php**
Risk	**High**

Fig. 25. Riesgo Alto.

Discusión

Vega detectó un formulario con un campo de entrada de contraseña que se envía a un objetivo inseguro (HTTP). Los valores de las contraseñas nunca deben enviarse en claro a través de canales inseguros. Esta vulnerabilidad podría dar lugar a la divulgación no autorizada de contraseñas a atacantes de red pasivos.

Impacto

Vega ha detectado un formulario que puede provocar el envío de una contraseña a través de un canal inseguro.
Esto podría dar lugar a la divulgación de contraseñas a los espías de la red.

Remediación

Las contraseñas nunca deben enviarse por texto sin cifrar. El formulario debe enviarse a un objetivo HTTPS[4].

Classification	Configuration Error
Resource	**Apache/2.4.6 (CentOS) PHP/7.3.19**
Method	**TRACE**
Risk	Medium

Fig. 25. Riesgo Medio II.

[3] Protocolo TLS (Transport Layer Security, seguridad de la capa de transporte)es una versión actualizada y más segura de SSL. Utilizan cifrado ECC, RSA o DSA. [8]

[4] HTTPS es la nueva versión del protocolo de transferencia de hipertexto (HTTP), la "S" al final quiere decir Seguro. [9]

Discusión

Se puede abusar de la compatibilidad con HTTP TRACE en escenarios en los que se ha encontrado una vulnerabilidad de secuencias de comandos entre sitios, pero no se puede explotar para recuperar los valores de las cookies porque las cookies de destino se establecen con el indicador HttpOnly. La bandera HttpOnly indica a los navegadores que no permitan el acceso a la cookie por Javascript. Si se encuentra una vulnerabilidad de secuencias de comandos entre sitios, pero la cookie de sesión está configurada HttpOnly, el soporte para HTTP TRACE abrirá una oportunidad para el robo de cookies.

Impacto

Permitir HTTP TRACE puede permitir el rastreo entre sitios.
Los atacantes pueden usar el rastreo entre sitios con secuencias de comandos entre sitios para recuperar el valor de las cookies HttpOnly.
Remediación

Para los servidores basados en Apache, la directiva TraceEnable se puede usar para deshabilitar la compatibilidad con HTTP TRACE.
Para los servidores basados en IIS, la configuración del registro EnableTraceMethod controla la compatibilidad con HTTP TRACE.

4. CONCLUSIONES

- Vega es una herramienta que nos permite detectar fácilmente vulnerabilidades en aplicaciones Web.
- La herramienta Vega está desarrollada en el lenguaje de programación Java por lo que funciona perfectamente en sistemas operativos tipo GNU/Linux y Windows
- Vega puede ser una buena alternativa a escáneres de pago. No da los mismos resultados pero es una excelente herramienta presente en Kali Linux5 y qué nos puede ayudar para encontrar vulnerabilidades web.
- El desarrollo e implementación de Vega se enfocó en las áreas que la empresa consideró primordiales en el proceso de comunicación interna las cuales son, comunicación, gestión documental, colaboración, aprendizaje, comenzando por la recolección de datos e identificando las vulnerabilidades necesarias para posteriormente definir los requerimientos del sistema en base a éstas.
- El reconocimiento de Vega que abordó este trabajo está enfocado hacia la gestión de la comunicación a través de aplicaciones web. Se identificaron y agruparon los principales requisitos en vulnerabilidad el cual contiene identificadores en base a los perfiles: páginas web
- En el análisis de las características de Vega sobresalen: la arquitectura el cual es una base para analizar las vulnerabilidades web; el gestor de menús y sus elementos que son independientes de la estructura del contenido; la variedad de extensiones disponibles. el diseño adaptativo que tienen las plantillas de vega.
- Los análisis de Vega de red realizados en un entorno corporativo, se mostrarán capturas con la información ya procesada y que se ha considerado de mayor importancia. No se adjunta toda la información, ya que, al realizar las pruebas sobre un entorno privado, por motivos confidenciales, podrían comprometer el estado de la empresa auditada.
- La herramienta Vega diseñada en este trabajo realiza los análisis en segundo plano, despreocupando al usuario final del conocimiento de las herramientas que se utilizan, así como de su funcionamiento, etc.; proporcionando una interfaz sencilla, fácil de utilizar, en la que cualquier usuario, puede realizar un análisis sin disponer de conocimientos en ese campo y visualizar la información de estos.
- Vega atenta contra la posibilidad de vulnerabilidad de implementar estos controles en forma adecuada, en particular la creciente complejidad y variedad de páginas web

[5] Kali Linux es la versión actualizada y optimizada de la distro BackTrack que tiene como objetivo principal facilitar las mejores herramientas para realizar auditoría de redes y seguridad informática.[10]

incrementa de la misma forma la variedad de puntos vulnerables y técnicas de ataque.

- El análisis de vulnerabilidades informáticas es una acción necesaria para toda aplicación web que desarrolle y comercialice sistemas informáticos. Para ello la Vega, debe tener como prioridad el poder garantizar la aplicación de normas de seguridad en todos sus dominios y aplicativo web.

REFERENCIAS

"Vega-Scanner", Subgraph.com, 2020. [Online]. Available: https://subgraph.com/vega/documentation/Vega-Scanner/index.en.html. [Ac-cessed: 13- Jul- 2020].

U. Murashka, "Vega - Scan For Security", Scan For Security, 2020. [Online]. Available: https://www.scanforsecurity.com/scanners/vega.html. [Accessed: 13- Jul- 2020].

"Listado de Paginas Web Vulnerables o con errores de SQL Injection", R4Z0R_BL4CK - Information Security & Risk, 2020. [Online]. Available: https://r4z0rbl4ck.wordpress.com/2018/10/01/listado-de-paginas-web-vulnerables-o-con-errores-de-sql-injection/. [Accessed: 13- Jul- 2020].

Picartell. "Analizar las vulnerabilidades de cualquier sistema web con VEGA en el sistema operativo Kali Linux" YouTube, 2016 [Video file]. Available: https://youtu.be/k4PsXD-P6pI. [Accessed: 13- Jul- 2020].

"SQL Injection | OWASP", Owasp.org, 2020. [Online]. Available: https://owasp.org/www-community/attacks/SQL_Injection. [Accessed: 18- Jul- 2020].

"Cross Site Scripting (XSS) Software Attack | OWASP Foundation", Owasp.org, 2020. [Online]. Available: https://owasp.org/www-community/attacks/xss/. [Ac-cessed: 18- Jul- 2020].

"JDK vs. JRE", uqbar-wiki, 2020. [Online]. Available: http://wiki.uqbar.org/wiki/articles/jdkVsJre.ht [Accessed: 18- Jul- 2020].

"¿Qué son SSL, TLS y HTTPS?", ¿Qué son SSL, TLS y HTTPS?, 2020. [Online]. Available: https://www.websecurity.digicert.com/es/es/security-topics/what-is-ssl-tls-https. [Accessed: 19- Jul- 2020].

"¿Qué es HTTPS?", Pickaweb, 2020. [Online]. Available: https://www.pickaweb.es/ayuda/que-es-https/. [Accessed: 19- Jul- 2020].

"Qué es Kali Linux y qué puedes hacer con él", ComputerHoy, 2020. [Online]. Available: https://computerhoy.com/paso-a-paso/software/que-es-kali-linux-que-puedes-hacer-41671. [Accessed: 19- Jul- 2020].