UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

OCTUBRE 2019 - MARZO 2020

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS

TEMA:

Análisis de vulnerabilidades de la pagina web de la “Unidad Educativa Babahoyo" en la ciudad de Babahoyo

EGRESADO:

Jhonny Mora Manobanda

TUTORA:

ING. Maria Gonzales. MSC.

AÑO 2020

INTRODUCCION

La “Unidad Educativa Babahoyo” es una institución educativa que se encuentra ubicada en la ciudad de Babahoyo y brinda a sus estudiantes educación básica y de bachillerato, esta posee un sitio web del cual estudiantes y docentes hacen uso de la misma para acceder a información de la institución.

Este caso de estudio está enfocado al análisis de las diferentes vulnerabilidades que existen en la página web de la institución y que ponen en riesgo la información que allí se encuentra alojada, tanto de estudiante como de docentes y de la misma institución, que al no contar con medidas de seguridad esta puede llegar a ser fácilmente vulnerada.

Esta investigación se apoya del método analítico, ya que este método permite recopilar la información de una forma más detalladla ayudando a presentar las vulnerabilidades que se encuentren en este sitio web, debido a las carencias de seguridad que esta presenta. La línea de investigación al que va dirigido este caso de estudio es desarrollo de sistemas de la información, comunicación y emprendimiento, empresariales y tecnológicos mientras que su sublinea es desarrollo de sistemas informáticos.

El análisis de las vulnerabilidades que se muestra en esta investigación permitirá conocer las brechas de seguridad que el sitio web presenta y esto se realizará con ayuda de herramientas como “Observatory” que es un software de Mozilla que permite realizar un escaneo de seguridad a la página de la institución, para así saber cuáles son las falencias en términos de seguridad que esta presenta.

También se utilizará una herramienta web llamada “Quttera” que servirá para poder hallar posibles amenazas que comprometa la información de los usuarios que se encuentran navegando a través de la página web, cuando termina de realizar el análisis muestra si tiene o no archivos que sean maliciosos o que contenga links que se dirijan a sitios con phishing, etc.

Con la ayuda de estas herramientas y con el análisis de los resultados se podrá conocer el estado actual en términos de seguridad del portal web de la institución, teniendo así mayor oportunidad de tomar medidas que logren reducir el riesgo de la pérdida o manipulación de la información.

II. DESARROLLO

La “Unidad Educativa Babahoyo” establecida con el Código AMIE:12H00114 se encuentra ubicada en la provincia de los Ríos, Cantón Babahoyo, parroquia Camilo Ponce, en la Avenida Enrique Ponce Luque en el sector El Pireo, ofrece a la comunidad estudiantil educación básica y de Bachillerato, el tipo de unidad de esta institución educativa es Fiscal y cuenta con modalidad presencial y en jornada matutina y vespertina, cuenta con 123 Docentes y con 2592 estudiantes. (UBICA.EC, 2019)

Esta institución educativa cuenta con una página web que muestra a sus usuarios información de la institución, así como de la comunidad educativa, además se informa de nuevas actividades que se vaya a realizar dentro del planten entre otro tipo de información.

Es importantes que las unidades educativas cuenten con sitios web oficiales porque estos ofrecen la posibilidad de que las personas que formen parte de la institución se informen de manera oficial todos los comunicados que vaya a realizar, así como también es importante ya que permite facilitar procesos como la matriculación de los estudiantes ya que este planten actualmente cuenta con un sistema que registra mediante el portal web la información de los estudiantes que se van a matricular siendo esta un gran beneficio ya que antes la unidad educativa llevaba este tipo de procesos de forma manual haciendo que el proceso de matriculación tarde mucho más y se incrementaba el riesgo de que la información este mal registrada.

Otro de los beneficios que representa tener su sitio web en la unidad educativa es el hecho de poder mostrar la información a cualquier momento del día, siendo mucho más fácil para usuarios ya que también pueden acceder desde cualquier sitio que tenga acceso a internet.

Hoy en día es muy necesario que las instituciones educativas cuenten con sitios web que ayuden a los estudiantes en diversos servicios y a encontrar información que les sea útil, tanto a maestros como a estudiantes.

Así mismo es importante la seguridad con la que cuenta esta información ya que es muy necesario que los datos de los miembros de la institución se encuentren íntegros y no hayan sido borrados o manipulados.

Cada año el ataque a sitios web se incrementa. Según (Valle, 2020) solamente durante 2019 el buscador de Google registró más de 4,2 millones de noticias y páginas en las que se hablaba de ciberseguridad. Otros términos referidos a incidentes protagonistas del año, como ransomware, suman casi 12 millones de páginas.

Partiendo de la necesidad de asegurar la información, es importante que se realicen análisis de seguridad a los portales web, ya que esto ayuda a informar de una forma temprana cualquier riesgo y vulnerabilidad que tenga el sitio web, logrando así obtener información que permita realizar cambios en los sitios para que estos se encuentren más seguros.

Cada cierto tiempo se detectan nuevas formas de acceder a la información que los sitios web alojan, exponiendo esta información a personas que las usan de una forma malintencionada, secuestran la información para luego obtener beneficios de las mismas.

En el sitio web de la institución “Unidad Educativa Babahoyo” no se han realizado este tipo de análisis de seguridad que expongan los riegos a los que está expuesto, siendo esa la causa principal de este caso de estudio ya que está enfocado en las vulnerabilidades.

Para llevar a cabo el caso de estudio es necesario tener en claro algunos conceptos relacionados a la seguridad en páginas web que ayudarán a comprender si existen vulnerabilidades o no.

Uno de esos términos es el protocolo HTTP este un protocolo de la capa de aplicación para la transmisión de documentos hipermedia, como HTML. Fue diseñado para la comunicación entre los navegadores y servidores web. (Mozilla, HTTP, 2019)

Cabe mencionar que el protocolo HTTP es uno de los primeros protocolos con los que se contaba para la transferencia de información, pero tenía muchas vulnerabilidades antes de que se creará su hoy sustituto HTTPS que brinda más seguridad para la información que se envía desde un equipo a otro.

Por otra parte, también se tiene el protocolo HTTPS, que es un método para garantizar una comunicación segura entre el navegador de un usuario y un servidor web. se reconoce por un candado en la ventana del navegador, que indica que la conexión es segura. (Pickaweb, 2018)

Las siglas SSL, se trata de una tecnología estandarizada que permite cifrar el tráfico de datos entre un navegador web y un sitio web, protegiendo así la conexión. Esto impide que pueda ver o interceptar la información que se transmite de un punto a otro. (DigiCert, 2019)

Según (Nguyen, 2018) explica en su libro que Cross-site scripting (XSS) permiten a los agentes de amenaza para insertar y ejecutar código no autorizado en aplicaciones web, El éxito de los ataques XSS en los sitios web de registro de votantes pueden proporcionar al atacante el acceso no autorizado a la información de los votantes.

Otro aspecto importante de la seguridad web es el concepto de "social engineering" en efecto, la manipulación de los seres humanos que tienen la información, aprovechando su ingenuidad, su amabilidad o la confianza que a veces se deposita en un desconocido sin comprobar su identidad real, permite ponerse en contacto fácilmente con un actor de la red, haciéndose pasar, por ejemplo, por alguna otra persona. (Audit, 2018)

Es importante mencionar que durante el desarrollo se evidenció algunos problemas de seguridad en el sitio web de la Unidad Educativa Babahoyo es por esto que este caso de estudio se empleó la metodología de investigación descriptiva pues esta brinda la facilidad de poder diagnosticar, identificar y describir los diferentes problemas de seguridad encontrados en el portal web, así como también la carencia de certificados digitales, brindando un enfoque más general en términos de seguridad. También

Haciendo uso de la investigación cualitativa se pudo determinar las herramientas de las que se va hacer uso para nuestro análisis de vulnerabilidades como es Observatory esta una herramienta que evalúa de cero a cien y de la A a la F. Realizando 11 comprobaciones diferentes, como uso de cookies, redirección a HTTPS, protección contra Javascript modificados o XSS. Además de sus propios tests, integra análisis de otros servicios similares, como SSL Labs o Security Headers (HTTP). (López, 2016)

Ya que no hay forma en específico de determinar el nivel de riesgo de un sitio determinado mediante programación. Se puede evaluar los estándares de seguridad del sitio web, el portal web Observatory califica los sitios por igual es decir evalúa con los mismos parámetros a todas las páginas web, mostrando a los desarrolladores y administradores de los sitios web que estándares defendidos de seguridad se están cumpliendo y que no.

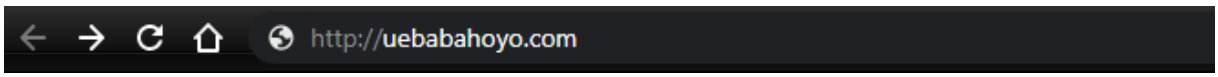
Las pruebas Observatorio son medidas preventivas que los sitios web deben realizar para evitar en lo posible ataques de cross-site scripting, ataques man-in-the-middle, la fuga de información entre dominios, el compromiso de las cookies, la red de distribución de contenidos (CDN), y los certificados emitidos de forma fraudulenta.

También se tiene la herramienta llamada Quttera que es una herramienta en la que ofrece un servicio similar a observatory en esta también se debe escribir la url en el campo para escanear. Cuando termina de analizar un sitio, muestra si está limpio o no, realiza una búsqueda de archivos maliciosos, posibles links fraudulentos que puedan ser phishing. (Jiménez, 2018)

Quttera ofrece servicios de ciberseguridad a plataformas tecnológica y brinda soluciones que permiten ayudar a las organizaciones a monitorear y proteger sus activos web informáticos del malware. Se especializan en la detectar posibles amenazas de seguridad basadas en la web como troyanos, gusanos, exploits, códigos de shell entre otros tipos de software malicioso.

Durante esta investigación se pudo apreciar que el sitio web cuenta no cuenta con el protocolo de seguridad https que es el protocolo más seguro y que cifra la información para mayor seguridad, careciendo de certificados digitales que comprueben la identidad de la página web resultando más fácil para sus atacantes poder crear el certificado que permita hacerse para pasar por el sitio web de la institución educativa.

Ilustración 1. Conexión no asegurada con el protocolo https



Fuente: *Jhonny Mora M.*

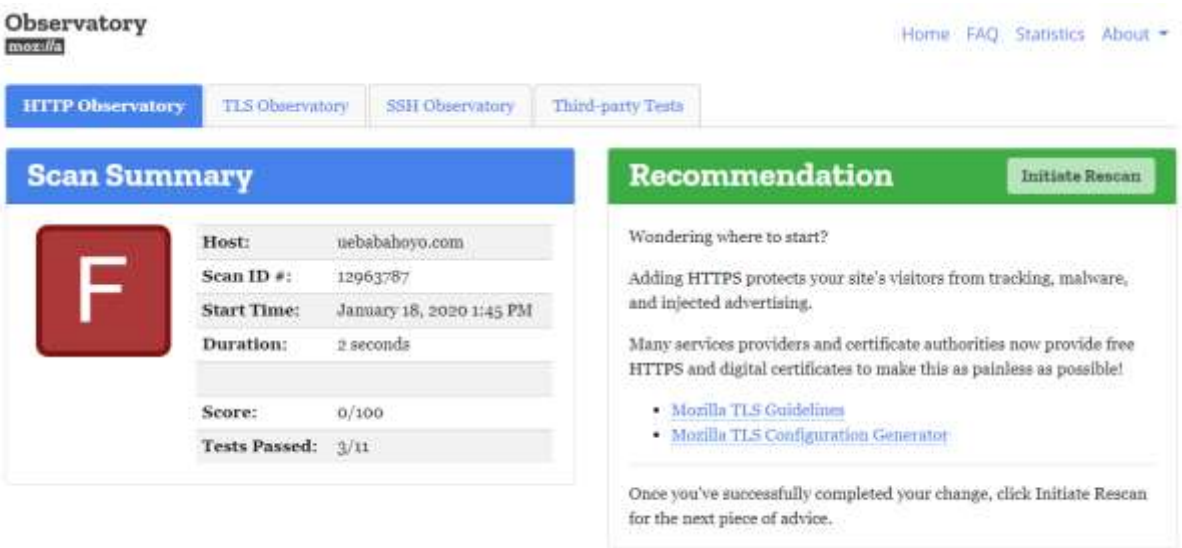
La primera herramienta que de la que se hará uso es de Observatory perteneciente a mozilla.org en su sitio principal muestra una caja de texto para poder ingresar la dirección que se quiere escanear y algunas opciones más que complementan el escaneo de forma más personalizada

Ilustración 2. Página de inicio de Observatory

Fuente: (Mozilla, Observatory, 2020).

Después de unos segundos de realizar la petición de escaneo muestra la información host del sitio web, el número de escaneo, la fecha en que se realizó y cuanto tardó en ejecutarse, así como también su respectiva calificación.

Ilustración 2. Página de inicio de Observatory



Fuente: (Mozilla, Observatory, 2020).

A continuación, se muestra los resultados de la evaluación que realiza en el test de la página, considerando que la evaluación se realiza tomando en cuenta los estándares de seguridad que debe tener una página para que su información se encuentre segura

Ilustración 3. Resultado del test

Test Scores

Test	Pass	Score	Reason	Info
Content Security Policy	✗	-25	Content Security Policy (CSP) header not implemented	ⓘ
Cookies	✗	-20	Cookies set without using the Secure flag or set over HTTP	ⓘ
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers	ⓘ
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header can't be implemented without HTTPS (optional)	ⓘ
HTTP Strict Transport Security	✗	-20	HTTP Strict Transport Security (HSTS) header cannot be set for sites not available over HTTPS	ⓘ
Redirection	✗	-20	Does not redirect to an HTTPS site	ⓘ
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)	ⓘ
Subresource Integrity	✗	-50	Subresource Integrity (SRI) not implemented, and external scripts are loaded over HTTP or use protocol-relative URLs via src="//..."	ⓘ
X-Content-Type-Options	✗	-5	X-Content-Type-Options header not implemented	ⓘ
X-Frame-Options	✗	-20	X-Frame-Options (XFO) header not implemented	ⓘ
X-XSS-Protection	✗	-10	X-XSS-Protection header not implemented	ⓘ

Fuente: (Mozilla, Observatory, 2020).

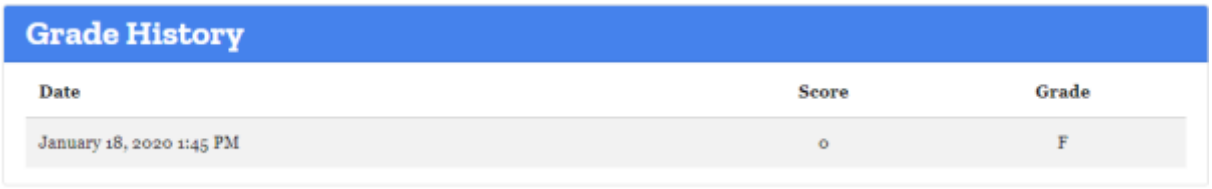
Análisis de los resultados del test en Observatory

Como se puede apreciar en los resultados del test la página no cuenta con política de seguridad de contenido esto es importante ya que les permite a los administradores del sitio web un detallado control sobre dónde se pueden cargar los recursos en su sitio. El uso de este encabezado es el mejor método para evitar vulnerabilidades de secuencias de comandos entre sitios (XSS). Debido a la dificultad de adaptar CSP a sitios web existentes, CSP es obligatorio para todos los sitios web nuevos y se recomienda a todos los sitios de alto riesgo existentes.

Las cookies se configuran sin usar la Secure bandera o se configuran a través de HTTP y esto no debe ser así ya que todas las cookies deben crearse de manera que su acceso sea lo más limitado posible disminuyendo la vulnerabilidad de scripting entre sitios (XSS), ya que estas cookies a menudo contienen identificadores de sesión u otra información confidencial.

Otro de los estándares de seguridad con los que no cuenta el sitio web es la Fijación de clave pública HTTP, Seguridad de transporte estricta de HTTP, No redirige a un sitio HTTPS, la Integridad de recursos no está implementada, y las secuencias de comandos externas se cargan a través de HTTP o utilizan URL relativas al protocolo a través de src="//...", El encabezado X-Content-Type-Options no está implementado, Cabecera X-Frame-Options (XFO) no implementada y la Cabecera X-XSS-Protección tampoco se encuentra implementada obteniendo así una puntuación de F

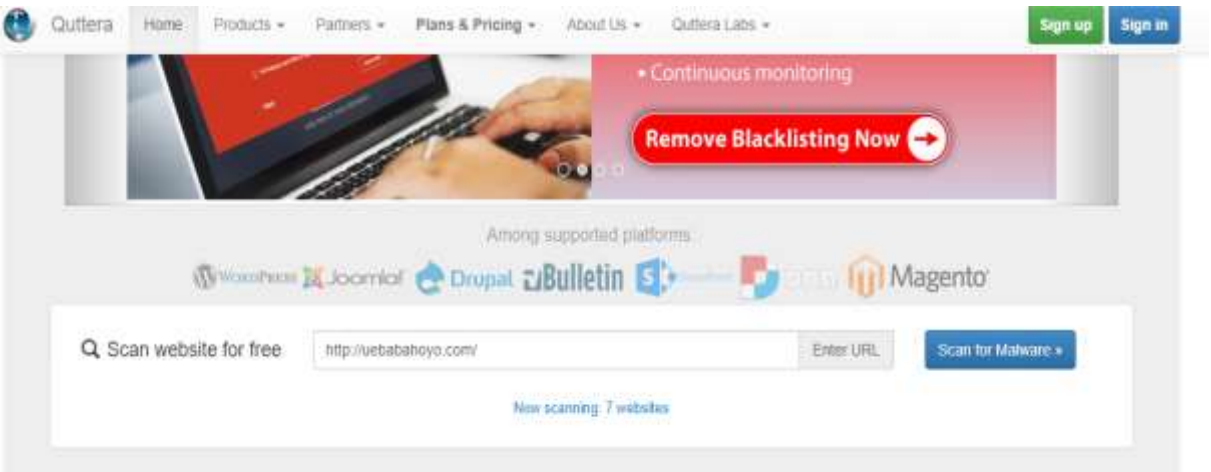
Ilustración 4. Calificación del test



Fuente: (Mozilla, Observatory, 2020).

La segunda herramienta a usarse es Qutera similar a la anterior realizará un análisis al sitio web en busca de vulnerabilidades y archivos maliciosos que se puedan encontrar alojados en el sitio web, cuenta con una página de inicio similar a la anterior herramienta ya que también tiene una caja de texto en el que se pondrá el link de la página que se va a realizar el escaneo.

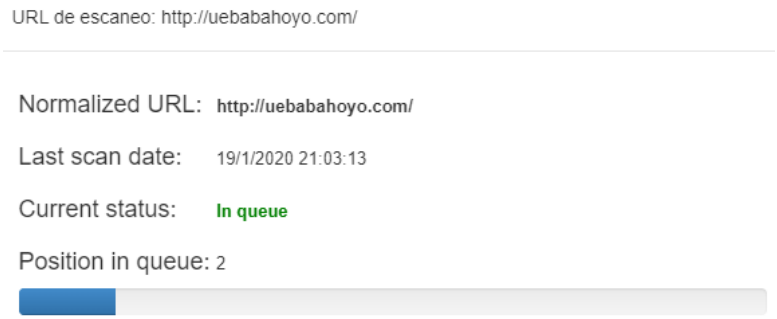
Ilustración 5. Página de inicio Quttera



Fuente: (Quttera, 2019)

Ingresado la url comienza a realizar el respectivo escaneo del sitio web, tardando no más de unos segundos en realizarse, esto varía dependiendo de la cantidad de enlaces y archivos que se encuentren alojados en la página web, mostrando también una barra de progreso en el que muestra en avance del escaneo.

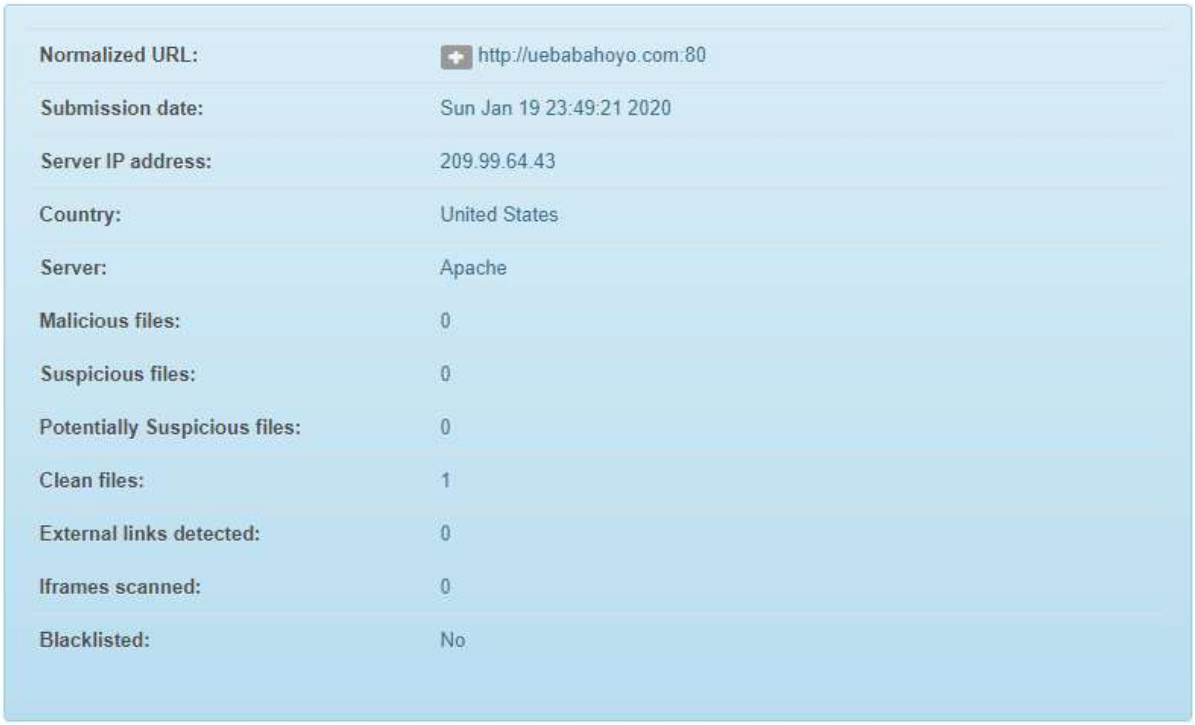
Ilustración 6. Resultados del escaneo en Quttera



Fuente: (Quttera, 2019)

Una vez concluido el proceso se procede a verificar los resultados que ofrece en el sitio web Quttera mostrando en la parte superior información básica del escaneo y en la parte inferior los resultados de la búsqueda de archivos maliciosos como potencialmente maliciosos.

Ilustración 6. Resultados del escaneo en Quttera



Normalized URL:	http://uebabahoyo.com:80
Submission date:	Sun Jan 19 23:49:21 2020
Server IP address:	209.99.64.43
Country:	United States
Server:	Apache
Malicious files:	0
Suspicious files:	0
Potentially Suspicious files:	0
Clean files:	1
External links detected:	0
Iframes scanned:	0
Blacklisted:	No

Fuente: (Quttera, 2019)

Análisis de los resultados del test en Quttera

Lo primero que muestra es información que se encontró en el sitio web analizado, como el url, la fecha en que se realizó en escaneo, su dirección ip, la ciudad, el servidor en el que está, en este caso es Apache, como se puede evidenciar también muestra que el sitio web no contiene archivos maliciosos

Tampoco archivos sospechosos ni potencialmente sospechosos, lo cual es positio para la página web ya que esto indica que no existen archivos que pueden producir daños o a sus usuarios, muestra que hay un archivo limpio y que no se ha detectado links externos, así como tampoco en lista negra.

Ilustración 7. Resultados del escaneo en Quttera

Fuente: (Quttera, 2019)

Análisis general de los resultados

Gracias a los resultados de la herramienta observatory se ha evidenciado que la página web de la unidad educativa Babahoyo no cuenta con los estándares adecuados para asegurar la integridad de sus datos obteniendo así una baja calificación en el aspecto de seguridad siendo vulnerable a posibles ataques futuros, de no aplicarse de aplicarse de forma inmediata estos estándares la página continuara de forma de forma continua en un estado de vulnerabilidad.

Mientras que gracias a la herramienta quttera se ha logrado ver que dentro de la página no existen archivos maliciosos que estén afectando al sitio web o a sus usuarios, es por ello que es recomendable que se continúe con continuos escaneos en búsqueda de estos archivos maliciosos ya que si no se aplican estándares de seguridad en el portal web es muy probable que logren ingresar archivos maliciosos a la página web de la institución.

III. CONCLUSIONES

Conforme al estudio realizado a la página web de la unidad educativa Babahoyo y en base al uso de las diferentes metodologías de investigación para la recolección de información, se ha obtenido las siguientes conclusiones:

- La página web carece de diferentes protocolos de seguridad y esto hace que se encuentre en un estado vulnerable ataques y que su información pueda ser accesible por atacantes informáticos.

- La unidad educativa no con cuenta con personal suficiente para la gestión y prevención de ataques informáticos puesto que solo existe un responsable que también ejerce el rol de docente de la institución.

- La página web de la institución no cuenta con infraestructura física propia para la gestión y mantenimiento de la paginas puesto que hay que realiza pagos a otras empresas para la debida gestión de su portal web y de su sistema.

Bibliografía

Audit, c. i. (2018). Seguridad informática - Hacking ético. Conocer el ataque para una mejor defensa (4a edición). Ediciones ENI, 2018.

DigiCert. (2019). *¿QUÉ SON SSL, TLS Y HTTPS?* Obtenido de https://www.digicert.com/es/what-is-ssl-tls-and-https-es/

Jiménez, J. (27 de Octubre de 2018). *redeszone.net*. Obtenido de Descubre si una web oculta algún tipo de amenaza con estas herramientas online: https://www.redeszone.net/2018/10/27/herramientas-online-analisis-paginas-web/

López, J. M. (22 de Diciembre de 2016). *Hipertextual SL*. Obtenido de Comprueba la seguridad de tu sitio web: https://hipertextual.com/2016/12/escaneres-online-seguridad-de-tu-pagina-web

Mozilla. (18 de Marzo de 2019). *HTTP*. Obtenido de https://developer.mozilla.org/es/docs/Web/HTTP

Mozilla. (2020). *Observatory*. Obtenido de https://observatory.mozilla.org/

Nguyen, N. H. (2018). Essential Cyber Security Handbook In Spanish. En *Manual esencial de seguridad cibernética en español* (pág. 383).

Pickaweb. (04 de Mayo de 2018). *¿Qué es HTTPS?* Obtenido de https://www.pickaweb.es/ayuda/que-es-https/

Quttera. (2019). *THREATSIGN! WEBSITE ANTI-MALWARE*. Obtenido de https://quttera.com/

UBICA.EC. (2019). *UNIDAD EDUCATIVA BABAHOYO en BABAHOYO*. Obtenido de https://www.ubica.ec/info/UNIDAD-EDUCATIVA-BABAHOYO

Valle, M. (16 de Enero de 2020). *Estos fueron los mayores ciberataques de 2019*. Obtenido de https://bitlifemedia.com/2020/01/estos-fueron-los-mayores-ciberataques-de-2019/

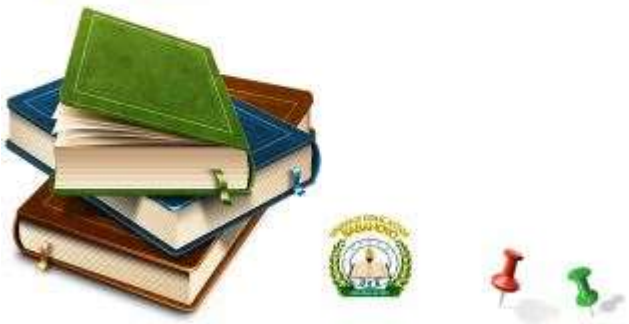
ANEXOS 1

Página web de la Unidad Educativa Babahoyo

Unidad Educativa Babahoyo... Educamos para la vida.

Unidad Educativa Babahoyo

Educamos para la vida.



Menú Principal

- Inicio
- Sistema BABAHOYO
- PASANTIAS
- DECE
- Clases Virtuales
- Correo Institucional
- Áreas de la Institución
- Videos
- Biblioteca Digital
- Temas de interés

URL: http://uebabahoyo.com/

ANEXO 2

ENTREVISTA AL RESPONSABLE DEL SITIO WEB DE LA UNIDAD EDUCATIVA BABAHOYO ING EDGAR CALDERON

1. **¿Qué función desempeña en la institución?**

   Docente y encargado del departamento de las tics

2. **¿La institución cuenta con personal técnico que le brinde asesoría en la seguridad del portal web?**

Sí, cuenta con asesoría de la empresa favola hosting

3. **¿Qué personas tienen acceso o permisos de administración a la página web?**

Solo en responsable del departamento de las TICS Ing. Edgar Calderón Sánchez

4. **¿Cómo calificaría usted la seguridad actual con la que cuenta la página web de la institución?**

   - Buena
   - Regular
   - Mala

5. **¿Alguna vez a recibido ataques informáticos la página web?**

   No ha se ha registrado ningún ataque

6. **¿Alguna vez ha fallado la infraestructura de la página web dejando de funcionar?**

Solo en caso de falta de pago del dominio que se utilizan

7. **¿Con qué herramientas cuentan la institución para asegurar o prevenir ataques a la página web?**

Wordfence Security y Vega.

8. **¿Se han realizado auditoras de seguridad a la página web y en qué año?**

Auditorías no, pero si revisiones preventivas.