Buen Data

buendata.com

moodle Partner
CERTIFIED SERVICES PROVIDER™

cel: 314 242 68 92
ramiro@buendata.com
soluciones@buendata.com

Segundo Diagnóstico de Plataformas LMS

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

moodle Partner
CERTIFIED SERVICES PROVIDER™

Segundo Diagnóstico plataformas LMS ESAP Contrato No BOG-1464-2024

Fecha informe:

Concepto: Informe

Cliente: Escuela Superior de Administración Pública

Escuela Superior de Administración Pública

Fecha de entrega: 30 de junio 2025

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

TABLA DE CONTENIDO

TABLA DE CONTENIDO 3
Índice de Imágenes 4
Índice de Tablas 5
SEGUNDO DIAGNÓSTICO ESAP 6
1. Diagnósticos de las plataformas LMS de la ESAP 6
1.1 Metodología Empleada 6
2. Recomendaciones segundo Diagnóstico Realizado 7
2.1 Recomendaciones segundo Diagnóstico Realizado Pregrado 7
2.1.1 Revisión de Plugins 7
2.1.2 Revisión de Análisis de seguridad 10
2.1.3 Revisión Estado del sistema 16
3. Recomendaciones segundo Diagnóstico Realizado Posgrado 17
3.1 Recomendaciones segundo Diagnóstico Realizado Pregrado 17
3.1.1 Revisión de Plugins 17
3.1.2 Revisión de Análisis de seguridad 19
3.1.3 Revisión Estado del sistema 27
4. Recomendaciones segundo Diagnóstico Realizado Extensión 28
4.1 Recomendaciones segundo Diagnóstico Realizado Extensión 28
4.1.1 Revisión de Plugins 28
4.1.2 Revisión de Plugins 29
4.1.3 Revisión Estado del sistema 38

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Índice de Imágenes

Ilustración 1. Revisión análisis de seguridad pregrado 10
Ilustración 2. Puertos Expuestos pregrado 13
Ilustración 3. Revisión estado del sistema pregrado 16
Ilustración 4. Revisión análisis posgrado 19
Ilustración 5. Revisión puertos expuestos posgrado 24
Ilustración 6. Plugins posgrado 29
Ilustración 7. Revisión expuestos Extensión 34

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Índice de Tablas

Tabla 1. Revisión Plugins Pregrado 9
Tabla 2. Revisión Plugins Posgrado 18
Tabla 3. Revisión Plugins Extensión 29

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

SEGUNDO DIAGNÓSTICO ESAP

Teniendo en cuenta el Plan de trabajo del Proyecto presentado por parte de Buen Data SAS, y según los ítems y actividades estipuladas bajo el marco del contrato No BOG-1464-2024. Se Presenta a continuación, el resultado del segundodiagnóstico frente a la estructura de la Esap y especialmente orientadas a Moodle.

1. Diagnósticos de las plataformas LMS de la ESAP

Servicio de diagnóstico de las plataformas actuales de LMS de la ESAP, las cuales se encuentran actualmente migradas a la nube dispuesto por la Universidad, para identificar que cumplen con los requisitos y estándares mínimos que permitan garantizar el correcto funcionamiento para los usuarios proyectados en cada una de ellas, de acuerdo a la planeación de las ofertas académicas de la ESAP.

Buen Data realizó a inicios del proyecto en diciembre de 2024, el diagnóstico de las plataformas de la ESAP.
Este documento comprende una segunda revisión realizada a la finalización del periodo de soporte, es importante, conocer que el primer diagnóstico insistía en la actualización de versión por lo que este documento es complementario del primer diagnóstico.

1.1 Metodología Empleada

Buen Data SAS realiza la revisión de las plataformas actualizadas, migradas a la nube de la entidad.

DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

2. Recomendaciones segundo Diagnóstico Realizado

El equipo de Buen Data ha encontrado las siguientes recomendaciones a nivel general de las instancias de Moodle, teniendo en cuenta de igual forma la actualización de versión de Moodle a su versión 4.5.

2.1 Recomendaciones segundo Diagnóstico Realizado Pregrado

A continuación, la revisión realizada la instancia de pregrado

2.1.1 Revisión de Plugins

Plugin	Versión Actual	Versión Moodle 4.5 LTS
Asistencia mod_attendance	2023041801 2023041801	2024072401 (2024072401)
Lista de verificación mod_checklist	4.1.0.2 2024051800	4.1.0.5 (2025041901)
Juego mod_game	2024-07-26 2024072600	2025-04-22 (2025042200)
Programador mod_scheduler	4.0.0 2023052300	No soportado, mal funcionamientos reportados en las versiones 4.3, 4.4 y 4.5
Ejercicio 2 de Turnitin mod_turnitintooltwo	4.1+ 2024080102	4.1+ (2025052901)
Accesibilidad block_accessibility	1.39.03 (Build - 2021092201) 2021092202	Sin mantenimiento

DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Estado de Finalización block_completion_progress	Version for Moodle 4.1 onwards 2023110100	Version for Moodle 4.5 onwards (2024100800)
Informes configurables block_configurable_reports	4.1.0 2023121803	4.5.0 (2024051300)
Dedicación al curso block_dedication	2023112001 2023112001	No se encuentra soportado aun oficialmente para 4.5
ReadSpeaker webReader block_readspeaker_embhl	2024041801	December release (Minor update) (2024121601)
Examview qformat_examview	2021051700	Eliminado del core (https://tracker.moodle.org/browse/MDL-72517)
Reunión de Teams atto_teamsmeeting	v1.2.7 2020032707	v1.2.7 (2020032707)
Formato de botones format_buttons	4.x 2022020801	4.x (2025051200)
Formato de Secciones Flexibles format_flexsections	4.1.0 2024052200	4.1.4 (2024120801)
Formato rejilla format_grid	401.2.3 2022112609	405.1.0 (2024101503)
Formato de temas de menú	michelle-4.0.2	michelle-4.4.1 (2025010201)

DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

format_menutopic	2023050703	
Temas en pestañas format_onetopic	4.1.12(PiedrasTeherán) 2022081612	4.4.05(LasAcacias) (2024050905)
Formato de cursos Edwiser format_remuiformat	4.1.7 2024042500	4.1.15 (2025050800)
Formato Ruta format_trail	4.2.0.0 2023060501	No soportado oficialmente
Moodle Benchmark report_benchmark	v1.5.1 2023012800	v1.5.3 (2025042700)
Plugin de control antiplagio Turnitin plagiarism_turnitin	3.5+ 2024072401	4.1+ (2025052901)
Páginas estáticas local_staticpage	v4.1-r2 2023010501	v4.5-r2 (2024100701)

Tabla 1. Revisión Plugins Pregrado

Los plugins de la Suite LXP no serán actualizados. Además, el plugin del WS SINU tampoco recibirá actualización, pero se sugiere validar su compatibilidad antes de la actualización, ya que en la versión 4.5 de Moodle se han introducido cambios heredados desde la versión 4.4 en los servicios web (WS).

BuenData
DOCUMENTO CONFIDENCIAL

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

2.1.2 Revisión de Análisis de seguridad

		Confidence			
		Alta	Media	Baja	Total
Risk	Alto	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)
	Medio	1 (14,3 %)	1 (14,3 %)	0 (0,0 %)	2 (28,6 %)
	Bajo	1 (14,3 %)	4 (57,1 %)	0 (0,0 %)	5 (71,4 %)
	Total	2 (28,6 %)	5 (71,4 %)	0 (0,0 %)	7 (100%)

Ilustración 1. Revisión análisis de seguridad pregrado

Alertas

Cabecera Política de seguridad de contenidos (CSP) no configurada

Etiquetas de alerta

- CWE-693
- OWASP_2021_A05
- OWASP_2017_A06

Descripción de la alerta

La Política de seguridad de contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos. Estos ataques se utilizan para todo, desde el robo de datos hasta la desfiguración del sitio o la distribución de malware. CSP proporciona un conjunto de encabezados HTTP estándar que permiten a los propietarios de sitios web declarar fuentes de contenido

DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

aprobadas que los navegadores deberían poder cargar en esa página; los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustados como applets de Java, ActiveX, archivos de audio y video.

Falta de cabecera Anti-Clickjacking

Etiquetas de alerta

- WSTG-v42-CLNT-09
- OWASP_2021_A05
- OWASP_2017_A06
- CWE-1021

Descripción de la alerta

La respuesta no protege contra ataques de "ClickJacking". Debes incluir Content-Security-Policy con la directiva "frame-ancestors" o X-Frame-Options.

Encabezado de seguridad de transporte estricto no establecido

Etiquetas de alerta

- OWASP_2021_A05
- OWASP_2017_A06
- CWE-319

Descripción de la alerta

HTTP Strict Transport Security (HSTS) es un mecanismo de política de seguridad web mediante el cual un servidor web declara que los agentes de usuario conformes (como un navegador web) deben interactuar con él utilizando únicamente conexiones HTTPS seguras (es decir, HTTP superpuesto a TLS/SSL). HSTS es un protocolo de seguimiento de estándares del IETF y se especifica en RFC 6797.

Cookie Sin Bandera de Seguridad

Etiquetas de alerta

- OWASP_2021_A05
- OWASP_2017_A06
- CWE-614

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

- WSTG-v42-SESS-02

Descripción de la alerta

Se ha establecido una cookie sin el indicador de seguridad, lo que significa que se puede acceder a la cookie a través de conexiones no cifradas.

Cookie con el atributo SameSite a Ninguno

Etiquetas de alerta

- OWASP_2021_A01
- OWASP_2017_A05
- WSTG-v42-SESS-02
- CWE-1275

Descripción de la alerta

Se ha establecido una cookie con su atributo SameSite establecido en «none», lo que significa que la cookie puede ser enviada como resultado de una solicitud 'cross-site'. El atributo SameSite es una medida efectiva para contrarrestar la falsificación de solicitudes cross-site, la inclusión de scripts cross-site y los ataques de sincronización.

Cookie sin el atributo SameSite

Etiquetas de alerta

- OWASP_2021_A01
- OWASP_2017_A05
- WSTG-v42-SESS-02
- CWE-1275

Descripción de la alerta

Se ha establecido una cookie sin el atributo SameSite, lo que significa que la cookie puede ser enviada como resultado de una solicitud 'cross-site'. El atributo SameSite es una medida eficaz para contrarrestar la falsificación de solicitudes entre sitios, la inclusión de scripts entre sitios y los ataques de sincronización.

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Falta encabezado X-Content-Type-Options

Etiquetas de alerta

- CWE-693
- OWASP_2021_A05
- OWASP_2017_A06

Descripción de la alerta

La cabecera Anti-MIME-Sniffing X-Content-Type-Options no se ha establecido en 'nosniff'. Esto permite que las versiones anteriores de Internet Explorer y Chrome realicen MIME-sniffing en el cuerpo de la respuesta, lo que puede provocar que el cuerpo de la respuesta se interprete y se muestre como un tipo de contenido distinto del tipo de contenido declarado. Las versiones actuales (principios de 2014) y heredadas de Firefox utilizarán el tipo de contenido declarado (si se establece uno), en lugar de realizar MIME-sniffing.

Puertos Expuestos

```
Nmap scan report for pregradoesap.esap.edu.co (35.239.82.41)
Host is up (0.096s latency).
rDNS record for 35.239.82.41: 41.82.239.35.bc.googleusercontent.com
Not shown: 65526 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE  SERVICE     VERSION
22/tcp    open   ssh         (protocol 2.0)
80/tcp    open   http
113/tcp   closed ident
443/tcp   open   ssl/https   Apache
541/tcp   open   reverse-ssl SSL/TLS ClientHello
4500/tcp  open   sae-urn?
8080/tcp  open   http-proxy
8445/tcp  open   ssl/copy?
10443/tcp open   ssl/unknown
```

Ilustración 2. Puertos Expuestos pregrado

El escaneo de red en el host pregradoesap.esap.edu.co (35.239.82.41) ha revelado múltiples servicios expuestos a Internet. Varios de estos servicios utilizan

DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

protocolos inseguros o son desconocidos, lo que representa un riesgo de seguridad significativo para el activo. Las vulnerabilidades identificadas se asocian principalmente con fallas criptográficas y misconfiguraciones de seguridad, incrementando la superficie de ataque del servidor.

Comunicación sin Cifrado (HTTP)

- **Puerto/Servicio:** 80/tcp (http)
- **Etiqueta de Alerta:** OWASP: A02:2021 - Cryptographic Failures
- **Descripción del Riesgo:** El servicio HTTP transmite toda la información, incluyendo posibles credenciales de inicio de sesión, datos personales o cookies de sesión, en texto plano. Un atacante con la capacidad de interceptar el tráfico (ataque Man-in-the-Middle) podría robar esta información fácilmente y obtener acceso no autorizado a cuentas de usuario o al sistema.
- **Recomendación:** Deshabilitar el puerto 80 o implementar una redirección permanente (301) a su contraparte segura HTTPS (puerto 443).

Punto de Acceso Administrativo Expuesto (SSH)

- **Puerto/Servicio:** 22/tcp (ssh)
- **Etiqueta de Alerta:** OWASP: A07:2021 - Identification and Authentication Failures
- **Descripción del Riesgo:** El puerto SSH está abierto a todo Internet, convirtiéndolo en un objetivo principal para ataques de fuerza bruta y de diccionario. Un atacante podría intentar adivinar contraseñas de forma automatizada para obtener control total del servidor.
- **Recomendación:**
    1. Restringir el acceso al puerto 22 únicamente a direcciones IP de confianza (lista blanca).
    2. Deshabilitar la autenticación por contraseña y exigir el uso de llaves criptográficas (SSH Keys).

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

3. Implementar software de bloqueo de IPs.

Servicios Desconocidos o No Estándar sobre SSL/TLS

- **Puertos/Servicios:**
  - 541/tcp (reverse-ssl)
  - 8445/tcp (ssl/copy?)
  - 10443/tcp (ssl/unknown)
- **Etiqueta de Alerta:** OWASP: A05:2021 - Security Misconfiguration
- **Descripción del Riesgo:** La presencia de múltiples servicios SSL/TLS en puertos no estándar y no identificados es una grave falla de configuración. Estos servicios podrían ser:
  - **Software sin gestionar:** Aplicaciones internas o de terceros que no están siendo monitoreadas ni actualizadas.
  - **Interfaces de administración ocultas:** Paneles de control que podrían otorgar acceso privilegiado.
  - **Backdoors o malware:** Un atacante podría haber instalado un canal de Mando y Control (C2) para mantener persistencia en el sistema. Estos puertos aumentan la superficie de ataque y operan fuera de los canales de monitoreo de seguridad habituales.
- **Recomendación:** Realizar una investigación inmediata para identificar la función de cada uno de estos servicios. Si no tienen un propósito de negocio legítimo y documentado, deben ser deshabilitados y bloqueados en el firewall a la brevedad posible.

Proxy HTTP Expuesto o Servicio Alternativo sin Cifrar

- **Puerto/Servicio:** 8080/tcp (http-proxy)
- **Etiqueta de Alerta:** OWASP: A05:2021 - Security Misconfiguration

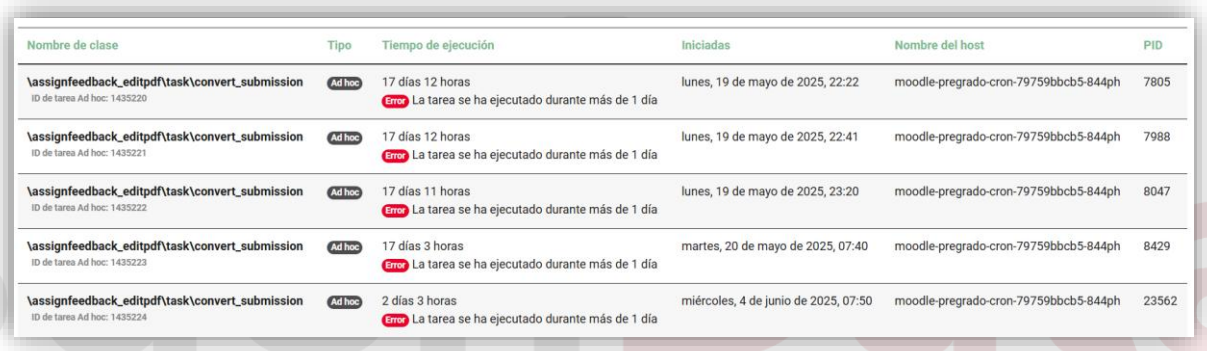
BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

- **Descripción del Riesgo:** Este puerto puede representar dos riesgos distintos:
    1. **Proxy Abierto:** Si está configurado como un proxy abierto, puede ser abusado por atacantes de todo el mundo para realizar actividades maliciosas (spam, ataques a otros sistemas) de forma anónima, haciendo que el tráfico malicioso parezca originarse desde su servidor.
    2. **Servidor Web Alternativo:** Si es un puerto alternativo para un servicio web, presenta los mismos riesgos de falta de cifrado que el puerto 80 (ver Alerta 1).
- **Recomendación:** Identificar el servicio. Si es un proxy, restringir su uso a una red interna o a usuarios autorizados. Si es un servidor web, asegurar la comunicación con TLS/SSL y considerar moverlo a un puerto estándar como el 443.

2.1.3 Revisión Estado del sistema

Retardo máximo en fallos de tareas	54793 tarea(s) fallidas
Cola de tareas Ad hoc	La tarea más antigua es 102 días



Nombre de clase	Tipo	Tiempo de ejecución	Iniciadas	Nombre del host	PID
\assignfeedback_editpdf\task\convert_submission ID de tarea Ad hoc: 1435220	Ad hoc	17 días 12 horas Error La tarea se ha ejecutado durante más de 1 día	lunes, 19 de mayo de 2025, 22:22	moodle-pregrado-cron-79759bbcb5-844ph	7805
\assignfeedback_editpdf\task\convert_submission ID de tarea Ad hoc: 1435221	Ad hoc	17 días 12 horas Error La tarea se ha ejecutado durante más de 1 día	lunes, 19 de mayo de 2025, 22:41	moodle-pregrado-cron-79759bbcb5-844ph	7988
\assignfeedback_editpdf\task\convert_submission ID de tarea Ad hoc: 1435222	Ad hoc	17 días 11 horas Error La tarea se ha ejecutado durante más de 1 día	lunes, 19 de mayo de 2025, 23:20	moodle-pregrado-cron-79759bbcb5-844ph	8047
\assignfeedback_editpdf\task\convert_submission ID de tarea Ad hoc: 1435223	Ad hoc	17 días 3 horas Error La tarea se ha ejecutado durante más de 1 día	martes, 20 de mayo de 2025, 07:40	moodle-pregrado-cron-79759bbcb5-844ph	8429
\assignfeedback_editpdf\task\convert_submission ID de tarea Ad hoc: 1435224	Ad hoc	2 días 3 horas Error La tarea se ha ejecutado durante más de 1 día	miércoles, 4 de junio de 2025, 07:50	moodle-pregrado-cron-79759bbcb5-844ph	23562

Ilustración 3. Revisión estado del sistema pregrado

DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

3. Recomendaciones segundo Diagnóstico Realizado Posgrado

El equipo de Buen Data ha encontrado las siguientes recomendaciones a nivel general de las instancias de Moodle, teniendo en cuenta de igual forma la actualización de versión de Moodle a su versión 4.5.

3.1 Recomendaciones segundo Diagnóstico Realizado Pregrado

A continuación, la revisión realizada la instancia de posgrado

3.1.1 Revisión de Plugins

Plugin	Versión Actual	Versión Moodle 4.5 LTS
Asistencia mod_attendance	2023041801 2023041801	2024072401 (2024072401)
Lista de verificación mod_checklist	4.1.0.2 2024051800	4.1.0.5 (2025041901)
Programador mod_scheduler	4.0.0 2023052300	No soportado, mal funcionamientos reportados en las versiones 4.3, 4.4 y 4.5
Accesibilidad block_accessibility	1.39.03 (Build - 2021092201) 2021092202	No soportado de forma oficial.
Estado de Finalización block_completion_progress	Version for Moodle 4.1 onwards 2025041400	Version for Moodle 4.5 onwards (2024100800)
Informes configurables	4.1.0	4.5.0 (2024051300)

DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

block_configurable_reports	2023121803	
Dedicación al curso block_dedication	2023112000	Soportado actualmente hasta la versión 4.4
Reunión de Teams atto_teamsmeeting	v1.2.7 2020032707	v1.2.7 (2020032707)
Fusión de cuentas de usuario tool_mergeusers	2023061900	2025020505 (Happy 2025) (2025020505)
Temas en pestañas format_onetopic	4.1.05(PiedrasTeherán) 2022081609	4.4.06(LasAcacias) (2024050906)
Benchmark (Comparativo) de Moodle report_benchmark	v1.5.1 2023012800	v1.5.3 (2025042700)
Ejercicio 2 de Turnitin mod_turnitintooltwo	4.1+ 2024080102	4.1+ (2025052901)
Turnitin Integrity plugin plagiarism_turnitinsim	v1.2 2023062901	v1.2 (2025052902)
Páginas estáticas local_staticpage	v4.2-r1 2023090100	v4.5-r2 (2024100701)

Tabla 2. Revisión Plugins Posgrado

Los plugins de la Suite LXP no serán actualizados. Además, el plugin del WS SINU tampoco recibirá actualización, pero se sugiere validar su compatibilidad antes de la actualización, ya que en la versión 4.5 de Moodle se han introducido cambios heredados desde la versión 4.4 en los servicios web (WS).

DOCUMENTO CONFIDENCIAL

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

3.1.2 Revisión de Análisis de seguridad

		Confidence			
		Alta	Media	Baja	Total
Risk	Alto	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)
	Medio	1 (9,1 %)	1 (9,1 %)	1 (9,1 %)	3 (27,3 %)
	Bajo	1 (9,1 %)	6 (54,5 %)	1 (9,1 %)	8 (72,7 %)
	Total	2 (18,2 %)	7 (63,6 %)	2 (18,2 %)	11 (100%)

Ilustración 4. Revisión análisis posgrado

Alertas

Cabecera Política de seguridad de contenidos (CSP) no configurada

Etiquetas de alerta

- OWASP_2021_A05
- POLÍTICA_QA_STD =
- POLÍTICA_PENTEST =
- CWE-693
- OWASP_2017_A06

Descripción de la alerta

La Política de seguridad de contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos. Estos ataques se utilizan para

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

todo, desde el robo de datos hasta la desfiguración del sitio o la distribución de malware. CSP proporciona un conjunto de encabezados HTTP estándar que permiten a los propietarios de sitios web declarar fuentes de contenido aprobadas que los navegadores deberían poder cargar en esa página; los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustados como applets de Java, ActiveX, archivos de audio y video.

Falta de cabecera Anti-Clickjacking

Etiquetas de alerta

- OWASP_2021_A05
- POLÍTICA_QA_STD =
- POLÍTICA_PENTEST =
- CWE-1021
- WSTG-v42-CLNT-09
- OWASP_2017_A06

Descripción de la alerta

La respuesta no protege contra ataques de "ClickJacking". Debes incluir Content-Security-Policy con la directiva "frame-ancestors" o X-Frame-Options.

Encabezado de seguridad de transporte estricto no establecido

Etiquetas de alerta

- OWASP_2021_A05
- POLÍTICA_QA_STD =
- POLÍTICA_PENTEST =
- CWE-319
- OWASP_2017_A06

Descripción de la alerta

HTTP Strict Transport Security (HSTS) es un mecanismo de política de seguridad web mediante el cual un servidor web declara que los agentes de usuario conformes (como un navegador web) deben interactuar con él utilizando únicamente conexiones HTTPS seguras (es decir, HTTP superpuesto a TLS/SSL).

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

HSTS es un protocolo de seguimiento de estándares del IETF y se especifica en RFC 6797.

Cookie Sin Flag HttpOnly

Etiquetas de alerta

- CWE-1004
- OWASP_2021_A05
- POLÍTICA_QA_STD =
- WSTG-v42-SESS-02
- POLÍTICA_PENTEST =
- OWASP_2017_A06
- ESTÁNDAR DE DESVÍO DE POLÍTICA

Descripción de la alerta

Se ha establecido una cookie sin el flag HttpOnly, lo que significa que JavaScript puede acceder a la cookie. Si un script malicioso puede ser ejecutado en esta página, entonces la cookie será accesible y puede ser transmitida a otro sitio. Si se trata de una cookie de sesión, el secuestro de sesión puede ser posible.

Cookie Sin Bandera de Seguridad

Etiquetas de alerta

- OWASP_2021_A05
- POLÍTICA_QA_STD =
- CWE-614
- WSTG-v42-SESS-02
- POLÍTICA_PENTEST =
- OWASP_2017_A06
- ESTÁNDAR DE DESVÍO DE POLÍTICA

Descripción de la alerta

Se ha establecido una cookie sin el indicador de seguridad, lo que significa que se puede acceder a la cookie a través de conexiones no cifradas.

DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Cookie con el atributo SameSite a Ninguno

Etiquetas de alerta

- OWASP_2021_A01
- POLÍTICA_QA_STD =
- WSTG-v42-SESS-02
- POLÍTICA_PENTEST =
- CWE-1275
- OWASP_2017_A05
- ESTÁNDAR DE DESVÍO DE POLÍTICA

Descripción de la alerta

Se ha establecido una cookie con su atributo SameSite establecido en «none», lo que significa que la cookie puede ser enviada como resultado de una solicitud 'cross-site'. El atributo SameSite es una medida efectiva para contrarrestar la falsificación de solicitudes cross-site, la inclusión de scripts cross-site y los ataques de sincronización.

Cookie sin el atributo SameSite

Etiquetas de alerta

- OWASP_2021_A01
- POLÍTICA_QA_STD =
- WSTG-v42-SESS-02
- POLÍTICA_PENTEST =
- CWE-1275
- OWASP_2017_A05
- ESTÁNDAR DE DESVÍO DE POLÍTICA

Falta encabezado X-Content-Type-Options

Etiquetas de alerta

- OWASP_2021_A05
- POLÍTICA_QA_STD
- POLÍTICA_PENTEST
- CWE-693

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

- OWASP_2017_A06

Descripción de la alerta

La cabecera Anti-MIME-Sniffing X-Content-Type-Options no se ha establecido en 'nosniff'. Esto permite que las versiones anteriores de Internet Explorer y Chrome realicen MIME-sniffing en el cuerpo de la respuesta, lo que puede provocar que el cuerpo de la respuesta se interprete y se muestre como un tipo de contenido distinto del tipo de contenido declarado. Las versiones actuales (principios de 2014) y heredadas de Firefox utilizarán el tipo de contenido declarado (si se establece uno), en lugar de realizar MIME-sniffing.

Gran redirección detectada (posible fuga de información confidencial)

Etiquetas de alerta

- OWASP_2021_A04
- POLÍTICA_PENTEST
- WSTG-v42-INFO-05
- OWASP_2017_A03
- CWE-201

Descripción de la alerta

El servidor ha respondido con una redirección que parece proporcionar una respuesta larga. Esto puede indicar que aunque el servidor envió una redirección, también respondió con el contenido del cuerpo (que puede incluir detalles confidenciales, PII, etc.).

Puertos Expuestos

```
Nmap scan report for posgradoesap.esap.edu.co (35.239.82.41)
Host is up (0.099s latency).
rDNS record for 35.239.82.41: 41.82.239.35.bc.googleusercontent.com
Not shown: 65527 filtered ports
PORT      STATE  SERVICE     VERSION
22/tcp    open   ssh         (protocol 2.0)
80/tcp    open   http
113/tcp   closed ident
443/tcp   open   ssl/https   Apache
541/tcp   open   reverse-ssl SSL/TLS ClientHello
8080/tcp  open   http-proxy
8445/tcp  open   ssl/copy?
10443/tcp open   ssl/unknown
```

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Ilustración 5. Revisión puertos expuestos posgrado

El servidor posgradoesap.esap.edu.co tiene varios servicios legítimos (SSH, HTTP, HTTPS con Apache), pero también una serie de puertos SSL/TLS no estándar (541, 8445, 10443) con servicios desconocidos o poco claros. Además, el puerto 8080 (proxy HTTP) también es un punto de atención.
Estos puertos no estándar y desconocidos aumentan significativamente la superficie de ataque y representan el mayor riesgo. Podrían ser aplicaciones desatendidas, interfaces de administración ocultas o incluso indicativos de una posible intrusión. Una investigación profunda de estos servicios es fundamental para determinar su propósito y asegurar el host.

Análisis de Puertos Abiertos y sus Implicaciones:

Punto de Acceso Administrativo Expuesto (SSH)

- **Puerto/Servicio:** 22/tcp (ssh)
- **Estado:** open
- **Versión:** (protocol 2.0)
- **Etiqueta de Alerta:** OWASP: A07:2021 - Identification and Authentication Failures
- **Descripción del Riesgo:** El puerto SSH está abierto a todo Internet, convirtiéndolo en un objetivo principal para ataques de fuerza bruta y de diccionario. Un atacante podría intentar adivinar contraseñas de forma automatizada para obtener control total del servidor.
- **Recomendación:**
    - Restringir el acceso al puerto 22 únicamente a direcciones IP de confianza (lista blanca).
    - Deshabilitar la autenticación por contraseña y exigir el uso de llaves criptográficas (SSH Keys).

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

- Implementar software de bloqueo de IPs (e.g., fail2ban) para mitigar ataques de fuerza bruta.

Comunicación sin Cifrado (HTTP)

- **Puerto/Servicio:** 80/tcp (http)
- **Estado:** open
- **Etiqueta de Alerta:** OWASP: A02:2021 - Cryptographic Failures
- **Descripción del Riesgo:** El servicio HTTP transmite toda la información, incluyendo posibles credenciales de inicio de sesión, datos personales o cookies de sesión, en texto plano. Un atacante con la capacidad de interceptar el tráfico (ataque Man-in-the-Middle) podría robar esta información fácilmente y obtener acceso no autorizado a cuentas de usuario o al sistema.
- **Recomendación:** Deshabilitar el puerto 80 o implementar una redirección permanente (301) a su contraparte segura HTTPS (puerto 443).

Servicio Web Cifrado (HTTPS)

- **Puerto/Servicio:** 443/tcp (ssl/https)
- **Estado:** open
- **Versión:** Apache
- **Etiqueta de Alerta:** OWASP: A02:2021 - Cryptographic Failures (Potencial, si la configuración es débil)
- **Descripción del Riesgo:** Aunque el uso de HTTPS es fundamental para el cifrado, la seguridad efectiva depende de la configuración de TLS/SSL (versiones de protocolo, suites de cifrado, gestión de certificados). Una configuración débil o desactualizada podría hacer que la comunicación sea vulnerable a ataques criptográficos.
- **Recomendación:**
  - Asegurar que el servidor web Apache esté configurado para utilizar las versiones más recientes y seguras de TLS (preferiblemente TLS 1.2 o TLS 1.3).

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

- Deshabilitar versiones de SSL/TLS obsoletas (TLS 1.0, 1.1, SSLv2, SSLv3).
- Configurar solo suites de cifrado fuertes y desechar las débiles.
- Mantener el certificado SSL/TLS válido, actualizado y emitido por una autoridad de certificación confiable.

Servicios Desconocidos o No Estándar sobre SSL/TLS

- **Puertos/Servicios:**
  - 541/tcp (reverse-ssl SSL/TLS ClientHello)
  - 8445/tcp (ssl/copy?)
  - 10443/tcp (ssl/unknown)
- **Estado:** open
- **Etiqueta de Alerta:** OWASP: A05:2021 - Security Misconfiguration
- **Descripción del Riesgo:** La presencia de múltiples servicios SSL/TLS en puertos no estándar y no identificados es una grave falla de configuración. Estos servicios podrían ser:
  - **Software sin gestionar:** Aplicaciones internas o de terceros que no están siendo monitoreadas ni actualizadas.
  - **Interfaces de administración ocultas:** Paneles de control que podrían otorgar acceso privilegiado si son vulnerables.
  - **Backdoors o malware:** Un atacante podría haber instalado un canal de Mando y Control (C2) para mantener persistencia en el sistema. Estos puertos aumentan la superficie de ataque y operan fuera de los canales de monitoreo de seguridad habituales, dificultando su detección y respuesta a incidentes.
- **Recomendación:** Realizar una investigación inmediata para identificar la función de cada uno de estos servicios. Si no tienen un propósito de negocio legítimo y documentado, deben ser deshabilitados y bloqueados en el firewall a la brevedad posible. Priorizar el análisis del puerto 10443 por su naturaleza "desconocida".

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Proxy HTTP Expuesto o Servicio Alternativo sin Cifrar

- **Puerto/Servicio:** 8080/tcp (http-proxy)
- **Estado:** open
- **Etiqueta de Alerta:** OWASP: A05:2021 - Security Misconfiguration
- **Descripción del Riesgo:** Este puerto puede representar dos riesgos distintos:
    - **Proxy Abierto:** Si está configurado como un proxy abierto, puede ser abusado por atacantes de todo el mundo para realizar actividades maliciosas (spam, ataques a otros sistemas) de forma anónima, haciendo que el tráfico malicioso parezca originarse desde su servidor.
    - **Servidor Web Alternativo:** Si es un puerto alternativo para un servicio web, presenta los mismos riesgos de falta de cifrado que el puerto 80 (ver Alerta 2).
- **Recomendación:** Identificar el servicio. Si es un proxy, restringir su uso a una red interna o a usuarios autorizados. Si es un servidor web, asegurar la comunicación con TLS/SSL y considerar moverlo a un puerto estándar como el 443 o asegurar que sea solo accesible internamente si no es para uso público.

3.1.3 Revisión Estado del sistema

Retardo máximo en fallos de tareas: 4 tarea(s) fallidas

Cola de tareas Ad hoc: La cola de tareas Ad hoc tiene 3 tareas

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

4. Recomendaciones segundo Diagnóstico Realizado Extensión

El equipo de Buen Data ha encontrado las siguientes recomendaciones a nivel general de las instancias de Moodle, teniendo en cuenta de igual forma la actualización de versión de Moodle a su versión 4.5.

4.1 Recomendaciones segundo Diagnóstico Realizado Extensión

A continuación, la revisión realizada la instancia de Extensión

4.1.1 Revisión de Plugins

Plugin	Versión Actual	Versión Moodle 4.5 LTS
H5P mod_hvp	1.27.2 2024120900	
Accesibilidad block_accessibility	1.39.03 (Build - 2021092201) 2021092202	
Informes configurables block_configurable_reports	3.9.0 2020110300	
ReadSpeaker webReader block_readspeaker_embhl	2023121201	
Fusión de cuentas de usuario tool_mergeusers	2023061900	
Formato rejilla format_grid	402.2.6 2023051011	

DOCUMENTO CONFIDENCIAL

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Temas en pestañas format_onetopic	4.1.05(PiedrasTeherán) 2022081609	
Benchmark (Comparativo) de Moodle report_benchmark	v1.5.1 2023012800	
Páginas estáticas local_staticpage	v4.2-r1 2023090100	

Tabla 3. Revisión Plugins Extensión

Los plugins de la Suite LXP no serán actualizados.

4.1.2 Revisión de Plugins

		Confidence			
		Alta	Media	Baja	Total
Risk	Alto	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)
	Medio	1 (9,1 %)	1 (9,1 %)	1 (9,1 %)	3 (27,3 %)
	Bajo	1 (9,1 %)	6 (54,5 %)	1 (9,1 %)	8 (72,7 %)
	Total	2 (18,2 %)	7 (63,6 %)	2 (18,2 %)	11 (100%)

Ilustración 6. Plugins posgrado

DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Alertas

Cabecera Content Security Policy (CSP) no configurada

Alert tags

- CWE-693
- OWASP_2021_A05
- OWASP_2017_A06
- POLICY_QA_STD
- POLICY_PENTEST

Alert description

La Política de seguridad de contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos. Estos ataques se utilizan para todo, desde el robo de datos hasta la desfiguración del sitio o la distribución de malware. CSP proporciona un conjunto de encabezados HTTP estándar que permiten a los propietarios de sitios web declarar fuentes de contenido aprobadas que los navegadores deberían poder cargar en esa página; los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustados como applets de Java, ActiveX, archivos de audio y video.

Falta de cabecera Anti-Clickjacking

Alert tags

- OWASP_2021_A05
- POLICY_QA_STD =
- POLICY_PENTEST =
- CWE-1021
- WSTG-v42-CLNT-09
- OWASP_2017_A06

Alert description

La respuesta no protege contra ataques de "ClickJacking". Debes incluir Content-Security-Policy con la directiva "frame-ancestors" o X-Frame-Options.

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Strict-Transport-Security Header No Establecido

Alert tags

- OWASP_2021_A05
- OWASP_2017_A06
- POLICY_QA_STD =
- POLICY_PENTEST =
- CWE-319

Alert description

HTTP Strict Transport Security (HSTS) es un mecanismo de política de seguridad web mediante el cual un servidor web declara que los agentes de usuario conformes (como un navegador web) deben interactuar con él utilizando únicamente conexiones HTTPS seguras (es decir, HTTP superpuesto a TLS/SSL). HSTS es un protocolo de seguimiento de estándares del IETF y se especifica en RFC 6797.

Cookie Sin Flag HttpOnly

Alert tags

- CWE-1004
- OWASP_2021_A05
- POLICY_QA_STD =
- WSTG-v42-SESS-02
- POLICY_PENTEST =
- OWASP_2017_A06
- POLICY_DEV_STD =

Alert description

Se ha establecido una cookie sin el flag HttpOnly, lo que significa que JavaScript puede acceder a la cookie. Si un script malicioso puede ser ejecutado en esta página, entonces la cookie será accesible y puede ser transmitida a otro sitio. Si se trata de una cookie de sesión, el secuestro de sesión puede ser posible.

Cookie Sin Flag de Seguridad

DOCUMENTO CONFIDENCIAL

Alert tags

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

- OWASP_2021_A05
- POLICY_QA_STD =
- CWE-614
- WSTG-v42-SESS-02
- POLICY_PENTEST =
- OWASP_2017_A06
- POLICY_DEV_STD =

Alert description

Se ha establecido una cookie sin el indicador de seguridad, lo que significa que se puede acceder a la cookie a través de conexiones no cifradas.

Cookie con el atributo SameSite a None

Alert tags

- OWASP_2021_A01
- POLICY_QA_STD =
- WSTG-v42-SESS-02
- POLICY_PENTEST =
- CWE-1275
- OWASP_2017_A05
- POLICY_DEV_STD =

Alert description

Se ha establecido una cookie con su atributo SameSite establecido en «none», lo que significa que la cookie puede ser enviada como resultado de una solicitud 'cross-site'. El atributo SameSite es una medida efectiva para contrarrestar la falsificación de peticiones cross-site, la inclusión de scripts cross-site y los ataques de sincronización.

Cookie sin el atributo SameSite

Alert tags

- OWASP_2021_A01
- POLICY_QA_STD =
- WSTG-v42-SESS-02

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

- POLICY_PENTEST =
- CWE-1275
- OWASP_2017_A05
- POLICY_DEV_STD =

Alert description

Se ha establecido una cookie sin el atributo SameSite, lo que significa que la cookie puede ser enviada como resultado de una solicitud 'cross-site'. El atributo SameSite es una medida eficaz para contrarrestar la falsificación de peticiones entre sitios, la inclusión de scripts entre sitios y los ataques de sincronización.

Falta encabezado X-Content-Type-Options

Alert tags

- CWE-693
- OWASP_2021_A05
- OWASP_2017_A06
- POLICY_QA_STD =
- POLICY_PENTEST =

Alert description

La cabecera Anti-MIME-Sniffing X-Content-Type-Options no se ha establecido en 'nosniff'. Esto permite que las versiones anteriores de Internet Explorer y Chrome realicen MIME-sniffing en el cuerpo de la respuesta, lo que puede provocar que el cuerpo dé la respuesta se interprete y se muestre como un tipo de contenido distinto del tipo de contenido declarado. Las versiones actuales (principios de 2014) y heredadas de Firefox utilizarán el tipo de contenido declarado (si se establece uno), en lugar de realizar MIME-sniffing.

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Puertos expuestos

```
Nmap scan report for extensionesap.esap.edu.co (35.239.82.41)
Host is up (0.099s latency).
rDNS record for 35.239.82.41: 41.82.239.35.bc.googleusercontent.com
Not shown: 65526 filtered ports
PORT      STATE  SERVICE     VERSION
22/tcp    open   ssh         (protocol 2.0)
80/tcp    open   http
113/tcp   closed ident
443/tcp   open   ssl/https   Apache
541/tcp   open   reverse-ssl SSL/TLS ClientHello
4500/tcp  open   sae-urn?
8080/tcp  open   http-proxy
8445/tcp  open   ssl/copy?
10443/tcp open   ssl/unknown
```

Ilustración 7. Revisión expuestos Extensión

El servidor muestra una combinación de servicios estándar y puertos inusuales, algunos de los cuales carecen de cifrado adecuado o son de naturaleza desconocida. Estas condiciones incrementan la superficie de ataque y sugieren posibles fallas de configuración y falta de visibilidad sobre los activos expuestos, requiriendo una investigación y remediación urgentes para mitigar riesgos críticos.

Punto de Acceso Administrativo Expuesto (SSH)

- **Puerto/Servicio:** 22/tcp (ssh)
- **Estado:** open
- **Versión:** (protocol 2.0)
- **Etiqueta de Alerta:** OWASP: A07:2021 - Identification and Authentication Failures
- **Descripción del Riesgo:** El puerto SSH está abierto a todo Internet, convirtiéndolo en un objetivo principal para ataques de fuerza bruta y de diccionario. Un atacante podría intentar adivinar credenciales de forma automatizada para obtener control total del servidor.
- **Recomendación:**

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

- Restringir el acceso al puerto 22 únicamente a direcciones IP de confianza (lista blanca) o redes específicas.
- Deshabilitar la autenticación por contraseña y exigir el uso de llaves criptográficas (SSH Keys) para un método de autenticación más robusto.
- Implementar software de bloqueo de IPs (e.g., fail2ban) para detectar y mitigar intentos de acceso no autorizado.

Comunicación sin Cifrado (HTTP)

- **Puerto/Servicio:** 80/tcp (http)
- **Estado:** open
- **Etiqueta de Alerta:** OWASP: A02:2021 - Cryptographic Failures
- **Descripción del Riesgo:** El servicio HTTP transmite toda la información (incluyendo posibles credenciales de inicio de sesión, datos personales o cookies de sesión) en texto plano. Esto significa que un atacante con la capacidad de interceptar el tráfico (ataque Man-in-the-Middle) podría robar esta información fácilmente y obtener acceso no autorizado a cuentas de usuario o al sistema.
- **Recomendación:** Deshabilitar el puerto 80 o implementar una redirección permanente (HTTP 301) a su contraparte segura HTTPS (puerto 443) para asegurar que todo el tráfico web sea cifrado.

Servicio Web Cifrado (HTTPS)

- **Puerto/Servicio:** 443/tcp (ssl/https)
- **Estado:** open
- **Versión:** Apache
- **Etiqueta de Alerta:** OWASP: A02:2021 - Cryptographic Failures (Potencial, si la configuración es débil)
- **Descripción del Riesgo:** Aunque el uso de HTTPS es una práctica esencial para la seguridad y el cifrado de datos, la fortaleza de la protección depende directamente de la configuración subyacente de TLS/SSL (versiones de protocolo soportadas, suites de cifrado permitidas, y la

BuenData
DOCUMENTO CONFIDENCIAL

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

gestión del certificado). Configuraciones débiles o desactualizadas pueden exponer el servidor a vulnerabilidades criptográficas conocidas.

- **Recomendación:**
    - Asegurar que el servidor web Apache esté configurado para utilizar solo las versiones más recientes y seguras de TLS (preferiblemente TLS 1.2 o TLS 1.3).
    - Deshabilitar versiones obsoletas de SSL/TLS (como TLS 1.0, 1.1, SSLv2, SSLv3).
    - Configurar solo suites de cifrado fuertes y seguras, y descartar las débiles o comprometidas.
    - Mantener el certificado SSL/TLS válido, actualizado y emitido por una autoridad de certificación reconocida y confiable.

Servicios Desconocidos o No Estándar sobre SSL/TLS

- **Puertos/Servicios:**
    - 541/tcp (reverse-ssl SSL/TLS ClientHello)
    - 8445/tcp (ssl/copy?)
    - 10443/tcp (ssl/unknown)
- **Estado:** open
- **Etiqueta de Alerta:** OWASP: A05:2021 - Security Misconfiguration
- **Descripción del Riesgo:** La presencia de múltiples servicios SSL/TLS en puertos no estándar y no identificados es una grave falla de configuración y un riesgo significativo. Estos servicios podrían ser:
    - **Software sin gestionar:** Aplicaciones internas o de terceros que no están siendo monitoreadas, parcheadas ni actualizadas regularmente.
    - **Interfaces de administración ocultas:** Paneles de control o APIs internas que, si no están debidamente protegidos, podrían otorgar acceso privilegiado a atacantes.

DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

- **Backdoors o malware:** Un atacante podría haber instalado un canal de Mando y Control (C2) para mantener persistencia y control sobre el sistema. Estos puertos aumentan la superficie de ataque del servidor y operan fuera de los canales de monitoreo de seguridad habituales, dificultando su detección y la respuesta a posibles incidentes.

- **Recomendación:** Realizar una investigación inmediata y exhaustiva para identificar la función y el propósito de cada uno de estos servicios. Si no tienen un propósito de negocio legítimo, claramente definido y documentado, deben ser deshabilitados y bloqueados en el firewall a la brevedad posible para reducir la superficie de ataque. El puerto 10443 es de particular preocupación por ser "desconocido".

Proxy HTTP Expuesto o Servicio Alternativo sin Cifrar

- **Puerto/Servicio:** 8080/tcp (http-proxy)
- **Estado:** open
- **Etiqueta de Alerta:** OWASP: A05:2021 - Security Misconfiguration
- **Descripción del Riesgo:** Este puerto puede representar dos riesgos distintos:
  - **Proxy Abierto:** Si está configurado como un proxy abierto, puede ser abusado por atacantes de todo el mundo para realizar actividades maliciosas (e.g., envío de spam, ataques de denegación de servicio a otros sistemas) de forma anónima, haciendo que el tráfico malicioso parezca originarse desde su servidor.
  - **Servidor Web Alternativo:** Si es un puerto alternativo para un servicio web no cifrado, presenta los mismos riesgos de falta de cifrado que el puerto 80 (ver Alerta 2), exponiendo la información transmitida.
- **Recomendación:** Identificar el servicio que se ejecuta en este puerto. Si es un proxy, restringir su uso estrictamente a una red interna o a usuarios autorizados mediante autenticación y listas blancas de IP. Si es un servidor web, asegurar la comunicación con TLS/SSL (HTTPS) y considerar moverlo

DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

a un puerto estándar como el 443, o asegurar que solo sea accesible internamente si su función no es pública.

Servicio sae-urn Expuesto

- **Puerto/Servicio:** 4500/tcp (sae-urn?)
- **Estado:** open
- **Etiqueta de Alerta:** OWASP: A05:2021 - Security Misconfiguration (Potencial)
- **Descripción del Riesgo:** Nmap identifica este puerto con el servicio sae-urn, aunque con un ? que indica incertidumbre sobre la versión o configuración exacta. Este puerto está asociado comúnmente con Internet Key Exchange (IKE) para IPsec, pero su exposición sin un propósito claro puede ser riesgosa. Un servicio no documentado o una versión vulnerable de un protocolo de seguridad puede ser explotado para reconocimiento o acceso no autorizado.
- **Recomendación:** Investigar el propósito de este servicio en el puerto 4500. Si no es esencial para el funcionamiento público o la seguridad del servidor, se recomienda deshabilitarlo o restringir su acceso mediante un firewall. Si es parte de una configuración de VPN/IPsec, asegurar que esté configurado con las mejores prácticas de seguridad, incluyendo la autenticación robusta y la actualización de cualquier software asociado.

4.1.3 Revisión Estado del sistema

Retardo máximo en fallos de tareas: 46 tarea(s) fallidas

Cola de tareas Ad hoc: La cola de tareas Ad hoc tiene 154 tareas

BuenData
DOCUMENTO CONFIDENCIAL

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Elaborado por:

Jean Ortega – Ingeniero Moodle
Leslie Martínez – Gestora de Proyecto

Revisado por:

Hemerson Carreño – Gerente de proyecto
Ramiro Guzmán – Gerente Comecial

(+57) 314 628 22 15 - 314 242 68 92 - 319 498 86

Comuníquese a través de los siguientes medios:

www.Buendata.com
Calle 65ª # 16 – 30 Bogotá -

leslie@buendata.com - soluciones@buendata.com – ramiro@buendata.com – hemerson@buendata.com

DOCUMENTO CONFIDENCIAL