OJSTI-CR-2026-01 v1.0

Informe de Caso: Evaluación Forense Anonimizada de Compromiso en el Servidor de un Entorno OJS

Una evaluación forense anonimizada de OJS que documenta compromiso server-side, actividad operativa de webshells, persistencia a nivel de host e impacto posterior sobre capas de aplicación, cuentas y datos.

Perfil del informe

TLP	CLEAR
SEVERIDAD	Alta
CONFIANZA	Alta
FECHA	14 Mar 2026
ANALISTA	Oscar Sandoval C., OJS One
CORPUS	Compromiso forense anonimizado y corpus de evidencia de apoyo
ESTADO	Final

Resumen ejecutivo

La evidencia analizada en este compromiso forense anonimizado, junto con el corpus de apoyo, sostiene con alta confianza la existencia de un compromiso real en el servidor que afectó a un entorno basado en OJS. Este documento funciona como el informe maestro del caso. Los informes analíticos asociados profundizan dimensiones técnicas específicas del mismo incidente, incluyendo componentes maliciosos, evidencia operativa en logs, persistencia, abuso de base de datos, alcance potencial del impacto e implicancias defensivas. El corpus combinado contiene múltiples artefactos PHP incompatibles con una operación legítima de OJS, incluyendo scripts con carga remota y ejecución basada en `eval()`, un componente de encubrimiento selectivo diseñado para alterar respuestas ante agentes de usuario vinculados a Google, un webshell con capacidad de carga y copias duplicadas de `phpFileManager` con autenticación embebida.

El caso también incluye una segunda capa de persistencia fuera de la raíz pública del sitio. Archivos de inicio de shell bajo la cuenta comprometida, incluyendo `.bashrc` y `.zshrc`, contenían un marcador `#defunct-kernel` seguido de una carga en shell codificada en base64. Ese contenido verificaba la existencia de un proceso `defunct` y, en ausencia del mismo, intentaba lanzar un componente oculto bajo `~/.config/htop/` mientras enmascaraba el nombre del proceso como `[mm_percpu_wq]`. Esto cambia de forma material la interpretación del incidente: el compromiso no estaba limitado a rutas de OJS ni a artefactos PHP expuestos públicamente.

El caso se ve reforzado por evidencia operativa. Los logs de acceso HTTP muestran interacción exitosa con **`sans.php`** en rutas web específicas, incluyendo navegación de `/home/` a través de funcionalidad de gestor de archivos. Los logs FTP registran actividad de escritura el 2026-03-05 desde una IP de origen contra múltiples instalaciones OJS y archivos sospechosos. La evidencia relacionada con SQL añade otra dimensión: el conjunto de respaldo documenta grupos de usuarios vinculados a spam y contaminación de perfiles, mientras que un informe separado de cuentas identifica 191 cuentas sospechosas, todas deshabilitadas a la fecha del reporte.

Tomados en conjunto, estos hallazgos sostienen una evaluación de alta confianza sobre compromiso técnico, capacidad operativa post-acceso, persistencia a nivel host y degradación de la confianza en los entornos OJS afectados. La evidencia no establece, por sí sola, un vector de acceso inicial definitivo, atribución de actor ni exfiltración de datos confirmada.

Por qué este informe importa

Este informe documenta un caso representativo de compromiso en OJS utilizando un corpus de evidencia combinado y no una sola familia de artefactos. Su valor está en mostrar que el incidente no puede reducirse a un webshell aislado ni a una sola entrada sospechosa en logs. En cambio, la actividad observada abarca componentes maliciosos del lado del servidor, evidencia operativa en logs, escrituras no autorizadas de archivos, persistencia en archivos de inicio de shell fuera del webroot e indicadores de contaminación a nivel de base de datos.

Para defensores, operadores de plataforma, equipos de respuesta a incidentes y grupos de investigación que monitorean amenazas contra sistemas de publicación académica, este caso demuestra cómo los entornos OJS pueden ser abusados mediante una combinación de encubrimiento selectivo, despliegue de webshells, herramientas de gestión de archivos y mecanismos de persistencia ubicados dentro de rutas legítimas de la aplicación.

Alcance y base de fuentes

Este informe se basa en dos corpus primarios de evidencia:

1. Un corpus de evidencia del entorno de hosting, que incluye contenido web, logs web, logs FTP y volcados SQL. 2. Un corpus de evidencia complementario, que incluye hallazgos resumidos, archivos maliciosos extraídos, indicadores de compromiso, hashes y un informe sobre cuentas sospechosas.
Los documentos fuente más relevantes para este informe ejecutivo son:

- Resumen interno de evidencia
- Nota interna de análisis del respaldo
- Evaluación interna de cuentas sospechosas

Este informe separa hechos observados de juicios analíticos y distingue entre evidencia observada directamente en el entorno de hosting y evidencia documentada en el corpus de respaldo.

Antecedentes y contexto del caso

El material revisado refleja compromiso en entornos OJS operados a través de múltiples rutas e instancias del sitio. La actividad es consistente con una operación posterior al acceso orientada a mantener control sobre el servidor, manipular respuestas web, habilitar operaciones remotas sobre archivos e introducir o sostener contenido malicioso adicional.
El caso es relevante porque el corpus de evidencia muestra más de un tipo de capacidad:

- encubrimiento selectivo del lado del servidor para agentes de usuario vinculados a Google;
- funcionalidad de webshell con capacidad de carga;
- puertas traseras de gestión de archivos con autenticación embebida;
- lógica de carga remota asociada a la entrega de contenido externo;
- actividad sospechosa de cuentas y perfiles en material de base de datos.

Esta amplitud de capacidades incrementa la confianza analítica en que los artefactos observados eran operativos y no meramente componentes preparados o abandonados.

Hallazgos clave

1. Se identificaron componentes PHP maliciosos en rutas de OJS con apariencia legítima e incompatibles con el comportamiento normal de la plataforma. 2. El corpus de respaldo confirma un componente de encubrimiento selectivo en **`bootstrap.inc.php`** que detecta agentes de usuario vinculados a Google y recupera contenido remoto desde un dominio externo. 3. El corpus de respaldo confirma un webshell con capacidad de carga en **`pdfJsViewer.php`**, activado por `qwerty303` y que muestra`XXxShell AccessxXX`. 4. El corpus de respaldo confirma puertas traseras duplicadas de `phpFileManager 1.7.9` con credenciales embebidas en **`UserHandlerr.php`** y **`sans.php`**. 5. El corpus del hosting confirma de forma independiente scripts adicionales con carga remota y copias de gestores de archivos bajo rutas OJS activas, incluyendo`/tools/uplaodsers.php`, `/templates/manageIssues/DebugFilter.php`, `/tools/Index.php`, `/tools/SearchIndex.php`, `/pages/manager/sans.php`, `/api/v1/users/UserHandlerr.php`, `/api/v1/submissions/core.php` y `/controllers/modals/submissionMetadata/linkAction/sans.php`. 6. Los logs HTTP muestran uso activo y exitoso de **`sans.php`**, incluyendo una solicitud para enumerar`/home/` mediante operaciones de árbol del gestor de archivos. 7. Los logs FTP muestran actividad de escritura el 2026-03-05 sobre varias rutas OJS y artefactos sospechosos desde una sola IP de origen. 8. La evidencia relacionada con base de datos dentro del corpus de respaldo documenta usuarios y perfiles vinculados a spam, y un informe separado identifica 191 cuentas sospechosas, todas deshabilitadas a la fecha del reporte.

Visión general de la evidencia

1. Encubrimiento selectivo para agentes de usuario relacionados con Google

El archivo**`bootstrap.inc.php`** contiene una rutina compacta que verifica `HTTP_USER_AGENT` en busca de cadenas como `Googlebot`, `Google-Site-Verification` y `Google-InspectionTool`. Si encuentra coincidencia, recupera contenido remoto desde un dominio externo, imprime la respuesta y termina la ejecución. Esto es consistente con encubrimiento selectivo deliberado del lado del servidor y manipulación de la respuesta en función del agente de usuario.

2. Webshell con capacidad de carga

Artefacto `pdfJsViewer.php`
Ruta observada `/plugins/generic/pdfJsViewer/pdfJsViewer.php`
Evaluación Webshell con capacidad de carga, activado por `qwerty303`, que muestra`XXxShell AccessxXX` e intenta copiar contenido a la raíz de documentos del servidor.

Visión general de la evidencia

3. Puertas traseras embebidas de gestión de archivos

Artefacto `UserHandlerr.php`
Ruta observada `/api/v1/users/UserHandlerr.php`
Evaluación Gestor de archivos embebido con `auth_pass` hardcodeado, que se identifica como `phpFileManager 1.7.9`.
Duplicado relacionado `sans.php`
Ruta observada `/pages/manager/sans.php`
Evaluación Herramienta operativa duplicada con el mismo hash SHA-256, lo que indica despliegue repetido de la misma puerta trasera de gestión de archivos en rutas distintas.

4. Confirmación independiente desde el volcado del hosting

El corpus de evidencia del hosting proporciona confirmación independiente de que el compromiso era más amplio que lo observado en la muestra del respaldo. Múltiples rutas OJS activas contenían artefactos con capacidad de carga remota o funciones tipo shell.
Las rutas activas observadas incluyen:

- `/tools/uplaodsers.php`
- `/locale/cs_CZ/DebugIndex.php`
- `/templates/manageIssues/DebugFilter.php`
- `/plugins/reports/reviewReport/ReviewRen.inc.php`
- `/tools/SearchIndex.php`
- `/tools/Index.php`
- `/pages/manager/sans.php`
- `/api/v1/users/UserHandlerr.php`
- `/api/v1/submissions/core.php`

Varios de estos archivos mostraban lógica de recuperación remota combinada con ejecución basada en `eval()`. Tomados en conjunto, refuerzan que la técnica observada no estaba aislada a una sola familia de archivos ni a una ubicación acotada dentro de la aplicación.

5. Uso operativo confirmado en logs

La evidencia en logs HTTP muestra acceso exitoso repetido a `/pages/manager/sans.php` el 2026-03-07 desde una IP externa recurrente, culminando en una solicitud que enumera`/home/` a través de la API de árbol del gestor de archivos. Ese comportamiento es difícil de conciliar con un acceso benigno o accidental y respalda uso real por parte del operador.

Visión general de la evidencia

6. Escrituras de archivos vía FTP

La evidencia en logs FTP registra escrituras el 2026-03-05 sobre múltiples archivos**`config.inc.php`** y rutas sospechosas, incluyendo `/templates/user/founds.php`, **`rome-shell.php`** y archivos inusuales bajo ubicaciones públicas de imágenes y plugins. Incluso cuando esos artefactos exactos ya no están presentes, el log confirma actividad de escritura sobre ubicaciones sensibles.

7. Abuso vinculado a base de datos

El corpus de respaldo documenta 137 usuarios vinculados a spam y 149 entradas de perfil contaminadas, mientras que la evaluación interna de cuentas sospechosas identifica 191 cuentas sospechosas que coinciden con patrones específicos de registro malicioso, todas deshabilitadas al momento de publicación. Esto indica que el incidente afectó no solo la integridad del sistema de archivos, sino también la confianza a nivel de aplicación.

Evaluación analítica

La evidencia sostiene, con alta confianza, que los entornos OJS afectados fueron comprometidos técnicamente y que el compromiso incluyó capacidad operativa post-acceso. Este juicio se basa en la convergencia de cuatro categorías de evidencia:

- evidencia directa en código de componentes no legítimos del lado del servidor;
- confirmación independiente de esos componentes a través de más de un corpus;
- evidencia en logs que muestra uso activo de al menos un backdoor de gestión de archivos;
- evidencia en base de datos que muestra abuso de cuentas y perfiles consistente con contaminación de más largo plazo.

La mezcla de artefactos observada sugiere un patrón de intrusión orientado a la persistencia y a la flexibilidad operativa más que a una carga de propósito único. El encubrimiento selectivo permite presentar contenido específico a agentes vinculados a Google. La funcionalidad de carga habilitada por el webshell permite introducir nuevas cargas. Los gestores de archivos embebidos permiten explorar, modificar y posiblemente preparar archivos a través de la raíz pública del sitio y de directorios adyacentes. Los cargadores remotos reducen la necesidad de almacenar toda la lógica en disco y permiten refrescarla o reemplazarla desde infraestructura externa.

También existe un patrón temporal relevante. Los timestamps se agrupan alrededor de 2026-03-07, mientras que el volcado del hosting muestra actividad sospechosa de escritura vía FTP el 2026-03-05 y uso interactivo del shell el 2026-03-07. Esto no prueba una secuencia única e ininterrumpida, pero sí respalda una interpretación de compromiso activo durante ese período.

Lo que la evidencia no establece de forma concluyente es el mecanismo de acceso inicial. Las escrituras vía FTP son un indicador fuerte de colocación o modificación no autorizada de archivos, pero no demuestran por sí solas si el actor utilizó credenciales robadas, otro canal administrativo o un exploit previo. Del mismo modo, la evidencia respalda una posible exposición de materiales sensibles, pero no prueba exfiltración.

Evaluación MITRE ATT&CK

Este informe utiliza ATT&CK como una lente analítica estructurada y no como una afirmación de reconstrucción completa de la secuencia operativa del actor.

T1505.003

Técnica: Server Software Component: Web Shell
Táctica: Persistencia
Evaluación: Fuertemente respaldada
La evidencia respalda directamente capacidad de shell server-side a través de **`pdfJsViewer.php`**, **`UserHandlerr.php`**, **`sans.php`**, **`core.php`** y artefactos PHP adicionales con comportamiento tipo shell identificados en rutas OJS activas. Este mapeo se ve reforzado por evidencia operativa en logs que muestra interacción activa con al menos un backdoor de gestión de archivos.

T1059.006

Técnica: Command and Scripting Interpreter: PHP
Táctica: Ejecución
Evaluación: Respaldada
El compromiso dependió de scripts PHP maliciosos como capa de ejecución para encubrimiento selectivo, comportamiento de carga, recuperación remota y lógica de gestión de archivos. El caso, por tanto, respalda el uso de PHP como mecanismo práctico de ejecución del lado del servidor a través del cual operó la técnica observada.

T1105

Técnica: Ingress Tool Transfer
Táctica: Command and Control
Evaluación: Respaldada
La capacidad de carga expuesta por **`pdfJsViewer.php`** y la lógica de cargadores remotos que recuperaban material externo hacia el entorno comprometido respaldan este mapeo. La combinación indica más que simple colocación estática de archivos y refleja capacidad para introducir o refrescar herramientas tras el acceso.

T1036

Técnica: Masquerading
Táctica: Evasión de defensas
Evaluación: Respaldada
Este mapeo está respaldado por la colocación de archivos bajo rutas OJS con apariencia legítima, patrones de nombres que imitan componentes esperables de la aplicación y persistencia a nivel host que intentó presentar un proceso de espacio de usuario con un nombre de apariencia kernel. El compromiso mezcló repetidamente funcionalidad maliciosa dentro de estructuras ordinarias de aplicación y de cuenta.

T1136

Técnica: Create Account
Táctica: Persistencia
Evaluación: Confianza menor
Los grupos de cuentas sospechosas y la contaminación de perfiles respaldan la preocupación por la presencia de cuentas no autorizadas, pero el corpus actual no establece por completo el mecanismo de creación para cada una de las cuentas representadas en la evidencia relacionada con base de datos.

Evaluación Cyber Kill Chain

La evidencia respalda con mayor fuerza las siguientes fases:

- **Installation:** Confirmada por colocación de PHP malicioso, loaders remotos, lógica de cloaking y file managers embebidos en rutas accesibles vía web.

- **Command and Control / Operational Control:** Parcialmente respaldada por comportamiento de recuperación remota y uso activo de rutas de webshell. Aunque este caso no muestra beaconing clásico, sí muestra herramientas del lado del servidor controladas por el atacante y utilizadas de forma interactiva.

- **Actions on Objectives:** Parcialmente respaldada por actividad de gestión de archivos, manipulación selectiva de respuestas ante agentes vinculados a motores de búsqueda e indicadores de contaminación de base de datos asociados a contenido y cuentas vinculadas a spam.

Las fases anteriores de Delivery y Exploitation permanecen sin resolver, ya que el corpus actual no identifica de forma concluyente el mecanismo de acceso inicial.

Confianza, supuestos y limitaciones

Confianza: Alta

Este nivel de confianza se basa en corroboración entre tipos de evidencia independientes: código fuente, hashes, logs, timestamps y artefactos vinculados a base de datos.
Limitaciones principales:

- Parte del corpus proviene de respaldos y no de una adquisición forense en vivo.
- El caso combina más de un paquete de evidencia y, por ello, requiere separación cuidadosa de fuentes.
- Algunos hallazgos de base de datos indican claramente actividad sospechosa, pero no toda cuenta o perfil anómalo puede atribuirse con el mismo nivel de certeza a nivel ejecutivo.
- No es posible atribución definitiva a partir del material revisado.
- No existe prueba definitiva de exfiltración de datos en este informe.

Conclusión ejecutiva

OJSTI evalúa con alta confianza que los entornos OJS revisados fueron objeto de un compromiso real del lado del servidor. La evidencia es suficiente para clasificar el caso como un evento severo de integridad que involucró componentes PHP maliciosos, capacidad operativa de webshell, actividad no autorizada de modificación de archivos y contaminación a nivel de aplicación.
El incidente demuestra cómo los entornos OJS pueden ser abusados mediante un conjunto escalonado de técnicas del lado del servidor que incluye encubrimiento selectivo, persistencia basada en carga, herramientas embebidas de gestión de archivos, recuperación remota de cargas y actividad sospechosa de cuentas. Aunque la evidencia actual no resuelve por completo el acceso inicial, la identidad del actor ni una exfiltración confirmada, sí es más que suficiente para sostener una determinación técnica de compromiso y justificar informes adicionales específicos por tema.

¿Tu infraestructura OJS está comprometida?

Los indicadores de compromiso suelen permanecer dormidos u ocultos dentro de rutas legítimas de la aplicación y de mecanismos de persistencia a nivel de cuenta. OJS One ofrece evaluaciones especializadas de compromiso y respuesta a incidentes para instituciones académicas que operan entornos OJS.
Solicita una evaluación forense `contacto@ojsone.com` `https://ojsone.com/en/cybersecurity`

Apéndice: artefactos clave e IOCs de alto nivel

Artefactos clave

- **`bootstrap.inc.php`**
- `plugins/generic/pdfJsViewer/pdfJsViewer.php`

- `api/v1/users/UserHandlerr.php`
- `pages/manager/sans.php`
- `tools/uplaodsers.php`
- `templates/manageIssues/DebugFilter.php`
- `tools/Index.php`
- `tools/SearchIndex.php`
- `api/v1/submissions/core.php`
- `controllers/modals/submissionMetadata/linkAction/sans.php`

IOCs de alto nivel

- `qwerty303`
- `XXxShell AccessxXX`
- `phpFileManager 1.7.9`
- `Google-Site-Verification`
- una IP externa recurrente asociada a acceso al webshell
- una IP externa recurrente asociada a escrituras vía FTP
- dominios sospechosos en cuentas, incluyendo`domailnew`, `dfokamail`, `mailerokdf` y `checkyourform`

Sobre OJS One

OJS One es una empresa especializada en Open Journal Systems que presta servicios de infraestructura, soporte técnico, continuidad operativa y seguridad para entornos de publicación basados en OJS.

Su trabajo combina operación de plataforma con evaluación de compromiso, hardening, respuesta a incidentes y análisis aplicado a la integridad de entornos editoriales.

A través de OJSTI, OJS One produce documentación técnica que identifica patrones de compromiso, técnicas observadas y lecciones defensivas relevantes para instituciones académicas, equipos editoriales, proveedores de hosting y actores de seguridad que operan OJS.

Más información:**`ojsone.com`**