Módulo 4. ZAP / Burp CE

CÓRDOBA CREA FUTURO

1. Metodología

La metodología en pruebas de seguridad de aplicaciones web constituye el marco estructural que organiza las actividades de evaluación, definiendo cómo se planifican, ejecutan y documentan las pruebas. Según el OWASP Web Security Testing Guide (WSTG), la metodología proporciona un enfoque sistemático para identificar vulnerabilidades mediante fases claramente delimitadas, evitando la improvisación y garantizando consistencia en los resultados. En este sentido, la metodología no se limita al uso de herramientas como ZAP o Burp CE, sino que establece criterios sobre qué probar, cómo probar y bajo qué condiciones.

OWASP distingue distintos tipos de pruebas de seguridad según el nivel de conocimiento que el evaluador posee sobre el sistema objetivo: caja blanca, caja negra y caja gris. Estas categorías definen el contexto metodológico desde el cual se desarrolla la evaluación. La elección del enfoque determina el alcance de las pruebas, el tipo de información disponible y

la profundidad del análisis, influyendo directamente en la interpretación de los resultados obtenidos.

El modelo de caja negra se caracteriza por la ausencia de información interna sobre la aplicación. El evaluador actúa como un usuario externo sin conocimiento del código fuente o arquitectura interna. En contraste, el modelo de caja blanca implica acceso completo a información técnica, incluyendo código, configuraciones y diseño. Entre ambos extremos se ubica el enfoque de caja gris, en el cual el evaluador dispone de información parcial, como credenciales de usuario o documentación limitada, pero no acceso total al sistema.

PortSwigger describe el *grey box testing* como un enfoque que combina elementos de conocimiento interno y externo, permitiendo una evaluación más realista de escenarios donde el atacante posee cierto nivel de acceso o información previa. Este enfoque resulta especialmente relevante en pruebas de aplicaciones web, donde muchas vulnerabilidades solo pueden identificarse al interactuar con funcionalidades autenticadas o roles específicos. Desde el punto de vista metodológico, la caja gris equilibra profundidad técnica y realismo operativo.

La metodología también exige definir claramente el alcance de las pruebas antes de iniciar cualquier actividad técnica. El WSTG enfatiza que el alcance determina qué sistemas, dominios, funcionalidades y cuentas serán evaluados, evitando ambigüedades que puedan generar conflictos o riesgos legales. En este sentido, la metodología establece límites explícitos que orientan la ejecución de herramientas y técnicas de prueba.

Otro componente metodológico es la formalización de autorizaciones. Toda prueba de seguridad debe contar con aprobación explícita por parte del propietario del sistema. OWASP subraya que las pruebas sin autorización pueden interpretarse como actividades maliciosas. Por lo tanto, la metodología integra no solo aspectos técnicos, sino también consideraciones legales y administrativas que regulan la actividad de *testing*.

Finalmente, la ética constituye un principio transversal en la metodología de pruebas de seguridad. El evaluador debe actuar con responsabilidad, minimizando impactos operativos y protegiendo la confidencialidad de la información obtenida durante el proceso. La metodología no busca causar daño, sino identificar debilidades de manera controlada y documentada. En consecuencia, el enfoque metodológico integra estructura técnica, delimitación formal

y responsabilidad profesional como componentes inseparables del proceso de evaluación.

Caja gris

El enfoque de *caja gris* constituye un modelo metodológico intermedio dentro de las pruebas de seguridad en aplicaciones web. OWASP, al diferenciar los tipos de pruebas según el nivel de conocimiento del evaluador, ubica la caja gris entre los modelos de caja negra y caja blanca. En este esquema, el evaluador dispone de información parcial sobre la aplicación, lo que permite orientar las pruebas sin contar con acceso completo al código fuente o arquitectura interna.

A diferencia de la caja negra, donde el análisis se realiza desde la perspectiva de un atacante externo sin conocimiento previo, la caja gris incorpora ciertos elementos internos como credenciales de usuario, documentación limitada o conocimiento básico de la estructura del sistema. Este nivel intermedio de información no elimina la necesidad de descubrimiento, pero permite focalizar la evaluación en componentes específicos y escenarios autenticados.

PortSwigger describe el *grey box testing* como un enfoque que combina la perspectiva externa con cierto entendimiento del funcionamiento interno. Esto resulta

especialmente relevante en aplicaciones web modernas, donde muchas funcionalidades críticas solo están disponibles tras autenticación. La posibilidad de evaluar flujos autenticados amplía la capacidad de identificar vulnerabilidades relacionadas con control de acceso, manipulación de sesiones o exposición de datos sensibles.

Desde el punto de vista metodológico, la caja gris permite simular escenarios más realistas. En numerosos contextos, los ataques no provienen exclusivamente de actores completamente externos, sino de usuarios con credenciales válidas que intentan exceder sus permisos. El enfoque de caja gris facilita la evaluación de estos escenarios, permitiendo analizar comportamientos dentro de distintos roles definidos en la aplicación.

El OWASP Web Security Testing Guide enfatiza la importancia de estructurar las pruebas en fases sistemáticas que incluyan reconocimiento, mapeo de la aplicación, análisis de autenticación y evaluación de autorizaciones. En un contexto de caja gris, estas fases se desarrollan con mayor profundidad en áreas accesibles mediante las credenciales disponibles, lo que incrementa la cobertura del análisis sin requerir acceso total al código.

La disponibilidad parcial de información también introduce responsabilidades metodológicas adicionales. El evaluador debe utilizar la información proporcionada exclusivamente dentro del alcance autorizado, evitando extender el análisis más allá de los límites definidos. La metodología establece que el conocimiento interno no debe transformarse en una exploración ilimitada, sino en una herramienta para orientar el *testing*.

Desde la perspectiva técnica, herramientas como ZAP o Burp CE se integran dentro de este enfoque permitiendo interceptar, modificar y analizar solicitudes autenticadas. En un contexto de caja gris, estas herramientas se utilizan para observar cómo responde la aplicación ante variaciones controladas de parámetros, identificadores y encabezados, manteniendo coherencia con el modelo metodológico definido.

El enfoque de caja gris también influye en la interpretación de resultados. Dado que el evaluador posee cierto conocimiento del sistema, las vulnerabilidades detectadas pueden contextualizarse con mayor precisión, identificando no solo la debilidad técnica, sino también el impacto

potencial según los roles y permisos existentes. Esta contextualización mejora la calidad del análisis posterior.

La caja gris representa un equilibrio metodológico entre profundidad técnica y realismo operativo. Permite evaluar escenarios autenticados, analizar controles de acceso y explorar funcionalidades internas sin requerir acceso completo al código fuente. Integrado dentro de una metodología estructurada como la propuesta por OWASP, este enfoque amplía la capacidad de detección de vulnerabilidades manteniendo un marco controlado y autorizado de evaluación.

Alcance y exclusiones

La definición de alcance constituye uno de los primeros pasos formales dentro de una metodología de pruebas de seguridad. El OWASP Web Security Testing Guide establece que antes de ejecutar cualquier actividad técnica debe definirse con precisión qué sistemas, aplicaciones, dominios y funcionalidades serán evaluados. El alcance delimita el espacio autorizado de análisis y establece los límites dentro de los cuales el equipo de *testing* puede operar.

Desde una perspectiva metodológica, el alcance no es una descripción genérica del sistema, sino un documento

explícito que identifica activos concretos. Esto incluye direcciones IP, dominios específicos, subdominios, entornos de prueba o producción, APIs y cuentas autorizadas para evaluación. La precisión en esta definición evita ambigüedades que puedan generar interpretaciones erróneas durante la ejecución de pruebas con herramientas como ZAP o Burp CE.

El WSTG enfatiza que el alcance debe acordarse previamente entre las partes involucradas, incluyendo propietarios del sistema y equipo de pruebas. Este acuerdo formaliza qué activos pueden ser analizados y cuáles quedan fuera del proceso. La ausencia de una delimitación clara puede derivar en riesgos legales o en impactos operativos no previstos.

El concepto de exclusiones complementa la definición de alcance. No todos los componentes relacionados con una organización forman parte necesariamente de la evaluación. Las exclusiones establecen explícitamente qué sistemas, servicios o funcionalidades no deben ser sometidos a pruebas, aun cuando estén técnicamente accesibles. Esta diferenciación previene la ejecución de pruebas sobre infraestructuras críticas o sobre sistemas de terceros.

Desde el punto de vista técnico, el alcance influye directamente en la configuración de herramientas de

análisis. Por ejemplo, los escaneos automatizados deben restringirse a dominios y rutas autorizadas, evitando exploraciones fuera del perímetro definido. La metodología requiere que el evaluador configure correctamente las herramientas para respetar las delimitaciones acordadas.

El alcance también determina la profundidad de las pruebas. No es lo mismo evaluar únicamente funcionalidades públicas que incluir áreas autenticadas o múltiples roles de usuario. La definición inicial debe especificar si se realizarán pruebas de autenticación, autorización, manipulación de sesiones o análisis de lógica de negocio, ya que cada uno de estos aspectos implica un nivel distinto de interacción con el sistema.

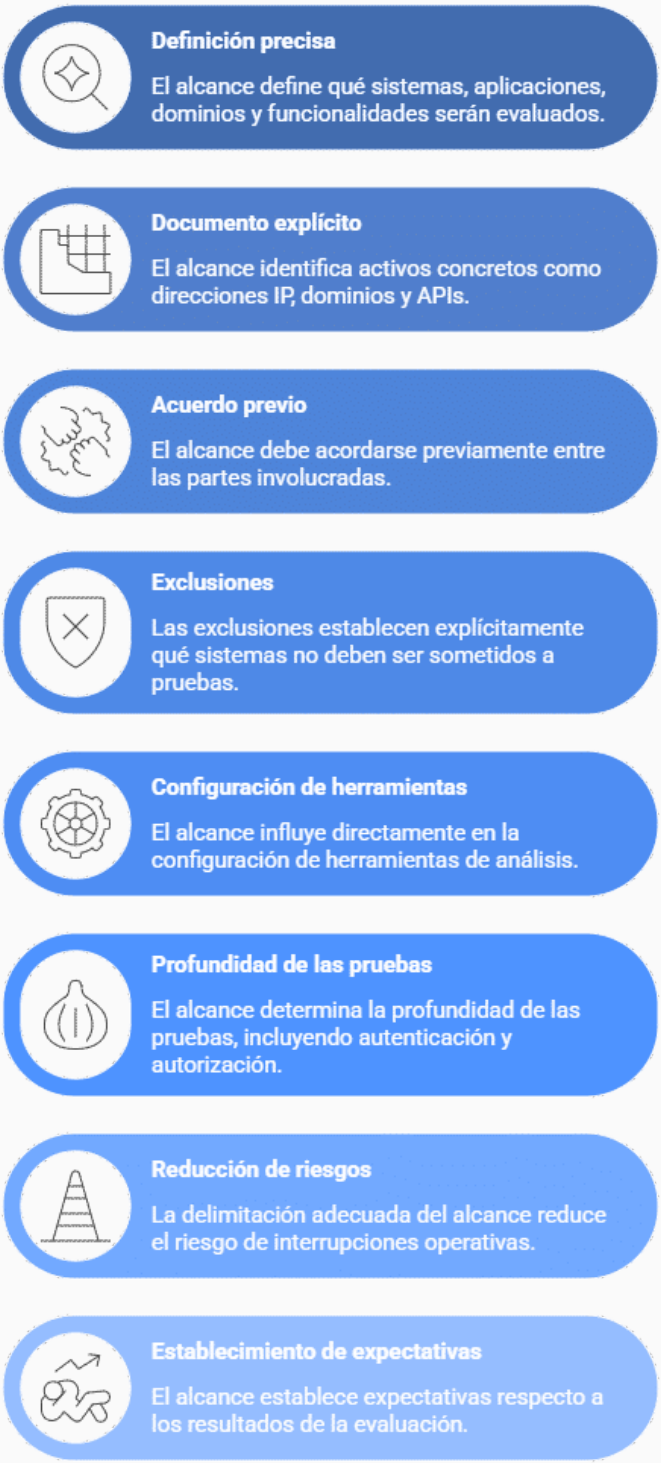
La delimitación adecuada del alcance reduce el riesgo de interrupciones operativas. Las pruebas de seguridad pueden generar cargas adicionales sobre el sistema o activar mecanismos de defensa como sistemas de detección de intrusiones. Al definir claramente los límites y comunicar el cronograma de pruebas, se minimiza la posibilidad de afectar la disponibilidad del servicio.

En términos metodológicos, el alcance también establece expectativas respecto a los resultados. Una evaluación limitada a ciertos componentes no puede interpretarse

como una revisión integral del sistema completo. Por ello, la documentación del alcance debe acompañar siempre los reportes finales, contextualizando las conclusiones obtenidas.

Figura 1. Componentes del alcance de las pruebas de seguridad

Componentes del alcance de las pruebas de seguridad



Fuente: elaboración propia.

El alcance y las exclusiones constituyen elementos estructurales dentro de la metodología de pruebas de seguridad. Su correcta definición garantiza que la evaluación se realice dentro de límites autorizados, técnicos y legales, evitando ambigüedades y reduciendo riesgos operativos. Integrado dentro del marco propuesto por OWASP, el *scoping* no es una formalidad administrativa, sino un componente central que condiciona toda la actividad de *testing*.

Autorizaciones

La autorización formal constituye un requisito previo indispensable en cualquier prueba de seguridad de aplicaciones web. El OWASP Web Security Testing Guide establece que ninguna actividad de *testing* debe iniciarse sin consentimiento explícito del propietario del sistema. La ausencia de autorización transforma una actividad técnica legítima en una posible conducta ilícita, independientemente de la intención del evaluador.

Desde una perspectiva metodológica, la autorización no es un trámite administrativo secundario, sino un componente estructural del proceso de evaluación. Debe especificar claramente qué activos pueden ser probados, durante qué período y bajo qué condiciones. Esta formalización delimita responsabilidades y protege tanto a la organización como al equipo de pruebas frente a malentendidos o interpretaciones erróneas.

El documento de *Rules of Engagement* (RoE), ampliamente difundido en la práctica profesional y desarrollado en marcos como los promovidos por SANS, establece las reglas operativas que regulan la ejecución del *testing*. Las RoE definen el alcance autorizado, las técnicas permitidas, los horarios de ejecución y los canales de comunicación en caso de incidentes. En este sentido, constituyen un acuerdo operativo que complementa la definición de alcance.

La autorización también debe especificar el nivel de intensidad permitido en las pruebas. No todas las organizaciones aceptan pruebas disruptivas o de denegación de servicio, por ejemplo. La claridad en este punto evita impactos no deseados sobre la disponibilidad del sistema. La metodología exige que el evaluador respete estrictamente las limitaciones establecidas en el acuerdo.

Desde el punto de vista legal, las pruebas sin autorización pueden vulnerar normativas relacionadas con acceso no autorizado a sistemas informáticos. Aunque el objetivo sea identificar vulnerabilidades, la intervención sobre un sistema sin permiso formal puede ser interpretada como actividad maliciosa. Por ello, la autorización escrita constituye un mecanismo de protección jurídica para ambas partes.

La formalización de autorizaciones también incluye la definición de cuentas y credenciales que podrán utilizarse durante la evaluación. En un contexto de pruebas de caja gris, por ejemplo, deben establecerse explícitamente los roles y perfiles disponibles para el evaluador. Esta delimitación impide el uso de accesos no contemplados en el acuerdo inicial.

El proceso de autorización debe incluir canales definidos para la notificación de hallazgos críticos. Las RoE suelen contemplar procedimientos de escalamiento en caso de descubrir vulnerabilidades de alto impacto. Esta previsión garantiza que los hallazgos se gestionen de manera controlada y responsable, minimizando riesgos operativos.

Desde la ética profesional, la autorización no habilita cualquier tipo de acción técnica. Incluso dentro del alcance acordado, el evaluador debe actuar con prudencia, evitando manipular datos sensibles más allá de lo necesario para demostrar la vulnerabilidad. La autorización establece el marco permitido, pero la responsabilidad técnica regula la forma en que se ejecutan las pruebas.

Las autorizaciones constituyen el fundamento legal, metodológico y ético de las pruebas de seguridad. A través de acuerdos formales y reglas de compromiso claramente definidas, se establece un entorno controlado para la evaluación. Integradas dentro de la metodología propuesta por OWASP, las autorizaciones garantizan que el *testing* se desarrolle dentro de límites legítimos y responsables.

Ética

La ética en pruebas de seguridad constituye el marco normativo que orienta la conducta del profesional encargado de evaluar sistemas y aplicaciones. El EC-Council, en su descripción del *ethical hacking*, define esta práctica como la identificación de vulnerabilidades con autorización previa y con el objetivo de mejorar la seguridad. En este

sentido, la diferencia entre un ataque malicioso y una prueba legítima no radica en la técnica empleada, sino en la intención, el consentimiento y el marco regulatorio que respalda la actividad.

Desde el punto de vista metodológico, la ética no es un complemento opcional del *testing*, sino un componente estructural. El evaluador debe actuar con responsabilidad, asegurando que cada acción técnica se encuentre dentro del alcance autorizado y que no genere daños innecesarios. La aplicación de herramientas como ZAP o Burp CE debe estar guiada por criterios de prudencia y proporcionalidad.

El concepto de *hacker* ético implica un compromiso explícito con la confidencialidad de la información obtenida durante el proceso de evaluación. En el transcurso de las pruebas pueden identificarse datos sensibles, configuraciones internas o credenciales. La ética profesional exige que esta información no sea divulgada ni utilizada para fines distintos a los acordados en el marco de la evaluación.

La responsabilidad ética también abarca la minimización de impactos operativos. Aunque las pruebas de seguridad buscan identificar debilidades, no deben comprometer la disponibilidad ni la integridad del sistema más allá de lo necesario para demostrar una vulnerabilidad. El evaluador

debe seleccionar técnicas que permitan evidenciar riesgos sin causar interrupciones indebidas.

Desde la perspectiva del comportamiento profesional, el *ethical hacking* implica transparencia en la comunicación de hallazgos. Los resultados deben documentarse de manera objetiva, evitando exageraciones o interpretaciones alarmistas. La finalidad del reporte es informar para mejorar la seguridad, no generar presión o exposición innecesaria.

La ética también exige respetar límites técnicos y organizativos. Si durante el *testing* se detectan activos fuera del alcance definido, el evaluador no debe analizarlos sin autorización adicional. El respeto por los límites acordados constituye una manifestación concreta del compromiso ético con la organización evaluada.

El enfoque del EC-Council destaca que el *ethical hacking* se fundamenta en la mejora continua de la seguridad. El profesional actúa como un agente de prevención, identificando debilidades antes de que sean explotadas por actores maliciosos. Esta orientación preventiva distingue la actividad legítima del uso indebido de técnicas de intrusión.

La formación ética también incluye el cumplimiento de normativas legales aplicables. Las pruebas deben alinearse con leyes de protección de datos, regulaciones sectoriales y políticas internas de la organización. La ética profesional no se limita a principios individuales, sino que se articula con marcos legales y regulatorios vigentes.

La ética en pruebas de seguridad integra consentimiento, responsabilidad, confidencialidad y respeto por los límites definidos. El *ethical hacking*, según el enfoque del EC-Council, se caracteriza por utilizar técnicas de evaluación con el propósito exclusivo de fortalecer la seguridad. Dentro de la metodología de *testing*, la ética no es una dimensión accesoria, sino el principio rector que legitima toda la actividad de evaluación.

CONTINUAR

2. Evidencias y reportes

La generación de evidencias y reportes constituye la etapa de formalización de los resultados obtenidos durante las pruebas de seguridad. Mientras la metodología organiza la ejecución técnica, el proceso de documentación transforma los hallazgos en información estructurada, verificable y comunicable. Sin esta etapa, la actividad de *testing* carecería de valor operativo, ya que las vulnerabilidades detectadas no podrían analizarse ni corregirse de manera sistemática.

Desde una perspectiva metodológica, la evidencia debe permitir reproducir el hallazgo identificado. Esto implica que cada vulnerabilidad documentada debe estar acompañada por información suficiente para que otro evaluador o el equipo técnico pueda replicar el comportamiento observado. La reproducibilidad constituye un criterio central de calidad en el reporte de seguridad.

La documentación de pruebas requiere precisión y control. Las evidencias no deben limitarse a descripciones generales,

sino incluir capturas, parámetros utilizados, solicitudes interceptadas, respuestas del servidor y contexto técnico. Esta estructuración permite diferenciar entre una observación superficial y un hallazgo técnicamente validado.

El reporte de seguridad también cumple una función comunicativa. No todos los destinatarios poseen el mismo nivel técnico; por ello, el documento debe organizar los hallazgos de forma clara, diferenciando descripción técnica, impacto potencial y recomendaciones. La claridad en la presentación facilita la toma de decisiones por parte de responsables técnicos y de gestión.

La clasificación de severidad constituye otro componente estructural del reporte. Las vulnerabilidades deben evaluarse según su impacto potencial, facilidad de explotación y alcance dentro del sistema. Esta categorización permite priorizar acciones correctivas, asignando recursos en función del riesgo asociado.

El proceso de reporte también debe incorporar un plan de remediación. Identificar una debilidad sin proponer una línea de acción correctiva limita la utilidad del informe. La remediación puede implicar ajustes de configuración, cambios en la lógica de autorización o implementación de controles adicionales, según la naturaleza del hallazgo.

Finalmente, la documentación de evidencias debe respetar criterios de integridad y confidencialidad. Las capturas y datos obtenidos durante la evaluación pueden contener información sensible. El almacenamiento y distribución del reporte deben gestionarse de manera controlada, garantizando que la información se utilice exclusivamente con fines de mejora de la seguridad.

Screenshots controlados

La captura de pantallas como evidencia en pruebas de seguridad constituye un recurso de documentación que debe aplicarse de manera estructurada y controlada. El OWASP Web Security Testing Guide, en su sección dedicada al *reporting*, establece que los hallazgos deben presentarse con evidencia clara, verificable y contextualizada. En este marco, las capturas no son elementos ilustrativos accesorios, sino soportes técnicos que permiten validar visualmente la existencia de una vulnerabilidad.

Desde una perspectiva metodológica, un *screenshot* controlado debe mostrar información suficiente para comprender el contexto del hallazgo. Esto implica incluir la URL visible, el parámetro modificado, el mensaje de error o la respuesta del sistema que evidencia la debilidad. Una

captura aislada, sin referencia contextual, carece de valor probatorio dentro del reporte.

El control en la generación de capturas también exige evitar la inclusión innecesaria de datos sensibles. Durante las pruebas pueden visualizarse credenciales, tokens de sesión o información personal. La documentación responsable implica anonimizar o difuminar datos que no sean necesarios para demostrar la vulnerabilidad. Este criterio se alinea con los principios de confidencialidad aplicables al proceso de *testing*.

Las capturas deben integrarse dentro de una narrativa técnica clara. OWASP enfatiza que el reporte debe permitir comprender cómo se identificó el hallazgo y qué pasos llevaron a su descubrimiento. El screenshot debe complementar la descripción escrita, no reemplazarla. La evidencia visual debe estar acompañada por explicación técnica que detalle el procedimiento realizado.

Desde el punto de vista de reproducibilidad, las capturas deben corresponder exactamente a los pasos descritos en el reporte. Si se modifica un parámetro específico mediante una herramienta como ZAP o Burp CE, la captura debe reflejar dicha modificación y la respuesta obtenida. La

coherencia entre descripción, pasos técnicos y evidencia visual fortalece la credibilidad del informe.

El control también implica estandarización. En un entorno profesional, las capturas deben seguir criterios uniformes de formato, nomenclatura y organización dentro del documento. Esto facilita la revisión por parte de equipos técnicos y evita confusiones. La estandarización convierte la evidencia visual en parte de una estructura documental coherente.

Desde una perspectiva técnica, las capturas pueden incluir tanto la vista del navegador como la visualización de solicitudes y respuestas interceptadas. En pruebas de seguridad web, muchas vulnerabilidades se evidencian en encabezados HTTP, códigos de estado o cuerpos de respuesta. La inclusión de estas evidencias técnicas refuerza la solidez del hallazgo.

El uso controlado de *screenshots* también reduce la ambigüedad. Una descripción textual puede interpretarse de distintas maneras, mientras que una captura precisa permite observar directamente el comportamiento del sistema. Esta visualización disminuye la posibilidad de malentendidos entre el evaluador y el equipo responsable de la remediación.

Los *screenshots* controlados constituyen un elemento técnico de soporte dentro del proceso de reporte de vulnerabilidades. Su valor radica en la claridad contextual, la coherencia con la descripción técnica, la protección de datos sensibles y la estandarización documental. Integrados correctamente en el informe, fortalecen la evidencia presentada y facilitan la comprensión y validación de los hallazgos detectados.

Tabla 1. Criterios para la elaboración de *screenshots* controlados en reportes de seguridad

Criterio	Descripción	Propósito en el reporte
Contexto visible	Inclusión de URL, entorno, rol de usuario y sección evaluada	Permitir identificar con precisión dónde ocurre la vulnerabilidad
Evidencia técnica clara	Visualización del parámetro modificado, solicitud HTTP o	Validar técnicamente el hallazgo

	respuesta del servidor	
Correspondencia con pasos descritos	La captura debe coincidir con los pasos detallados en el procedimiento	Garantizar reproducibilidad
Protección de datos sensibles	Anonimización de credenciales, tokens o información personal	Preservar confidencialidad
Integración narrativa	La imagen debe acompañarse de explicación técnica	Evitar ambigüedades interpretativas
Estandarización	Uso uniforme de formato, numeración y nomenclatura	Facilitar revisión y auditoría

Fuente: elaboracíon propia.

Reproducibilidad

La reproducibilidad constituye un criterio central en la documentación de pruebas de seguridad. Según el OWASP

Web Security Testing Guide, la evidencia presentada en un reporte debe permitir que otro evaluador o el equipo técnico pueda replicar el hallazgo siguiendo los pasos descritos. En este sentido, un hallazgo no se considera completamente validado si no puede reproducirse de manera consistente bajo las mismas condiciones.

Desde una perspectiva metodológica, la reproducibilidad implica detallar cada acción ejecutada durante la prueba. Esto incluye la descripción de la funcionalidad evaluada, los parámetros modificados, las solicitudes enviadas y las respuestas recibidas. La omisión de pasos intermedios debilita la capacidad de verificación y puede generar dudas respecto a la validez del hallazgo.

La documentación debe especificar el contexto en el cual se identificó la vulnerabilidad. Esto incluye el entorno probado, el tipo de cuenta utilizada, el rol asociado y cualquier condición previa necesaria para ejecutar la prueba. En entornos de caja gris, por ejemplo, la disponibilidad de credenciales específicas puede ser un factor determinante en la aparición del comportamiento observado.

El detalle técnico es un componente esencial para garantizar reproducibilidad. OWASP enfatiza que la documentación debe incluir datos suficientes como URLs exactas, métodos

HTTP utilizados, parámetros manipulados y códigos de respuesta del servidor. Sin estos elementos, el equipo responsable de la remediación podría no lograr replicar el escenario descrito.

La reproducibilidad también exige consistencia en los resultados. Si un comportamiento ocurre de manera intermitente o bajo condiciones no documentadas, debe aclararse en el reporte. La precisión en la descripción evita interpretaciones erróneas y facilita el análisis técnico posterior.

Desde el punto de vista de herramientas de *testing*, la reproducibilidad implica conservar registros técnicos como solicitudes interceptadas o exportaciones de tráfico HTTP. Estos registros pueden complementar la descripción escrita y fortalecer la evidencia presentada. La combinación de narrativa técnica y evidencia estructurada mejora la claridad del hallazgo.

La ausencia de reproducibilidad afecta la credibilidad del reporte. Un hallazgo que no puede verificarse genera

incertidumbre y retrasa la toma de decisiones. Por ello, la metodología de documentación propuesta por OWASP exige que cada vulnerabilidad incluya pasos claros para su replicación, evitando ambigüedades.

La reproducibilidad también facilita la validación posterior a la remediación. Una vez aplicada la corrección, el equipo técnico debe poder repetir los mismos pasos descritos para confirmar que la vulnerabilidad ha sido mitigada. Este ciclo de verificación fortalece el proceso de mejora continua en seguridad.

La reproducibilidad transforma un hallazgo técnico en evidencia verificable. Mediante la descripción detallada de pasos, contexto y resultados, se garantiza que el análisis pueda repetirse y validarse de manera independiente. Integrada dentro del marco de documentación del OWASP WSTG, la reproducibilidad constituye un criterio de calidad indispensable en los reportes de seguridad.

Severidad / impacto

La determinación de severidad e impacto constituye un componente estructural dentro del reporte de vulnerabilidades. No todas las debilidades identificadas poseen el mismo nivel de riesgo, por lo que resulta necesario

aplicar criterios sistemáticos para clasificarlas. La metodología de evaluación de riesgo propuesta por OWASP establece un modelo que considera probabilidad de explotación e impacto potencial, permitiendo asignar una valoración coherente y justificable.

El modelo de OWASP Risk Rating Methodology descompone el riesgo en dos grandes dimensiones: la probabilidad y el impacto. La probabilidad analiza factores como facilidad de explotación, nivel de acceso requerido y detectabilidad. El impacto, por su parte, evalúa las consecuencias técnicas y organizativas que podrían derivarse de la explotación de la vulnerabilidad. La combinación de ambas dimensiones permite categorizar el riesgo en niveles como bajo, medio o alto.

Desde la perspectiva técnica, el impacto puede afectar diferentes propiedades de seguridad, tales como confidencialidad, integridad y disponibilidad. Una vulnerabilidad que expone datos sensibles compromete la confidencialidad, mientras que una que permite modificar información afecta la integridad. Si la debilidad posibilita interrumpir el servicio, el impacto se relaciona con la disponibilidad. Esta clasificación facilita la comprensión estructurada del daño potencial.

El Common Vulnerability Scoring System (CVSS) versión 3.1 proporciona un marco estandarizado para cuantificar la severidad de vulnerabilidades. Aunque su especificación técnica es detallada, conceptualmente se basa en métricas que consideran el vector de ataque, la complejidad, los privilegios requeridos, la interacción del usuario y el impacto sobre confidencialidad, integridad y disponibilidad. Estas métricas generan una puntuación numérica que permite comparar vulnerabilidades de manera consistente.

Mientras OWASP propone una metodología adaptable al contexto organizacional, CVSS ofrece una escala cuantitativa estandarizada. Ambos enfoques pueden complementarse: la metodología de OWASP permite incorporar factores específicos del entorno evaluado, mientras que CVSS facilita la comunicación objetiva del nivel de severidad en términos comparables entre organizaciones.

La determinación de severidad no debe basarse únicamente en la existencia técnica de la vulnerabilidad, sino en su explotabilidad real dentro del contexto definido en el alcance. Una debilidad que requiere condiciones altamente improbables puede clasificarse con menor prioridad que otra fácilmente explotable. Por ello, la evaluación debe considerar tanto el escenario técnico como las condiciones operativas.

En el proceso de reporte, la severidad influye directamente en la priorización de remediaciones. Las vulnerabilidades clasificadas con mayor impacto o mayor probabilidad de explotación deben abordarse con prioridad superior. Esta jerarquización facilita la asignación eficiente de recursos y evita que debilidades críticas queden relegadas.

La documentación de la severidad también exige transparencia en los criterios utilizados. El reporte debe indicar qué metodología se aplicó y cómo se llegó a la clasificación asignada. Esta claridad fortalece la credibilidad del informe y permite que terceros comprendan el razonamiento detrás de la evaluación.

La determinación de severidad e impacto constituye un proceso analítico que transforma un hallazgo técnico en un riesgo evaluado. Mediante metodologías como la propuesta por OWASP y marcos estandarizados como CVSS v3.1, es posible clasificar vulnerabilidades de manera sistemática, priorizar acciones correctivas y comunicar el nivel de riesgo con claridad y coherencia.

Plan de remediación

El plan de remediación constituye la etapa final del proceso de reporte de vulnerabilidades, transformando los hallazgos identificados en acciones correctivas estructuradas. El NIST SP 800-61, en su guía de manejo de incidentes de seguridad informática, establece que la respuesta ante debilidades debe incluir fases organizadas que contemplen contención, erradicación y recuperación. En este sentido, la remediación no es una acción aislada, sino un proceso sistemático orientado a reducir riesgos identificados.

Desde una perspectiva metodológica, el plan de remediación debe vincularse directamente con la severidad asignada a cada hallazgo. Las vulnerabilidades clasificadas con mayor impacto o probabilidad de explotación requieren intervención prioritaria. Esta priorización permite gestionar recursos de manera organizada y evitar que debilidades críticas permanezcan expuestas por períodos prolongados.

El NIST enfatiza la importancia de documentar claramente las acciones correctivas propuestas. Cada vulnerabilidad debe estar acompañada por una descripción concreta de la medida recomendada, ya sea ajuste de configuración, fortalecimiento de controles de acceso, implementación de validaciones adicionales o actualización de componentes

afectados. La claridad en la recomendación facilita su implementación por parte del equipo técnico responsable.

El plan de remediación también debe contemplar responsabilidades asignadas. No basta con describir la acción técnica; es necesario definir qué equipo o rol será responsable de ejecutarla. Esta asignación contribuye a la trazabilidad del proceso y permite monitorear el avance de las correcciones dentro de un marco de gobernanza estructurado.

Desde la perspectiva de gestión de incidentes, la contención inmediata puede ser necesaria en casos de vulnerabilidades críticas. El NIST describe que, ante debilidades de alto riesgo, pueden adoptarse medidas temporales para reducir la exposición mientras se desarrolla una solución definitiva. Estas acciones transitorias forman parte del proceso de manejo estructurado del riesgo.

El plan de remediación también debe incluir plazos definidos. La ausencia de tiempos estimados puede generar postergaciones indefinidas en la corrección de debilidades. La planificación temporal contribuye a integrar la seguridad dentro del ciclo operativo regular de la organización, estableciendo compromisos claros de resolución.

Una vez aplicada la corrección, resulta necesario verificar su efectividad. El NIST destaca la importancia de validar que las acciones implementadas hayan mitigado adecuadamente el problema identificado. Esta verificación puede implicar repetir las pruebas descritas en el reporte original, asegurando que la vulnerabilidad ya no sea reproducible.

La documentación del proceso de remediación también cumple una función de aprendizaje organizacional. El análisis de causas permite identificar si la vulnerabilidad se originó en errores de configuración, debilidades en el control de acceso o deficiencias en procesos internos. Este aprendizaje contribuye a prevenir recurrencias futuras.

El plan de remediación transforma el reporte de vulnerabilidades en un proceso de mejora estructurada. Basado en lineamientos como los propuestos por el NIST SP 800-61, integra priorización, definición de acciones, asignación de responsabilidades, establecimiento de plazos y verificación posterior. De este modo, el ciclo de pruebas de seguridad se completa no solo con la identificación del riesgo, sino con su tratamiento organizado y documentado.

CONTINUAR

Referencias

EC-Council. (s. f.). *Ethical hacking overview*. https://www.eccouncil.org/ethical-hacking/

FIRST. (2019). *Common Vulnerability Scoring System v3.1: Specification document*. https://www.first.org/cvss/specification-document

National Institute of Standards and Technology. (2012). *Computer security incident handling guide* (SP 800-61 Rev. 2). https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

OWASP Foundation. (s. f.). *OWASP risk rating methodology*. https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

OWASP Foundation. (s. f.). *Testing methodology*. En OWASP Web Security Testing Guide. https://owasp.org/www-project-

web-security-testing-guide/

OWASP Foundation. (s. f.). *Types of security testing*. https://owasp.org/www-community/Types_of_Security_Testing

PortSwigger Ltd. (s. f.). *What is grey box testing?* https://portswigger.net/web-security

SANS Institute. (s. f.). *Rules of engagement* (RoE). https://www.sans.org/white-papers/

CONTINUAR