Puesta en producción Segura

Prueba de BurpSuitee

### 

| Índice |
| --- |
| [**Instalación**](#_i6jaj3qefdlr) **2**  [**Interceptar peticiones**](#_tiua41k5cvk3) **2**  [Proxy](#_tiua41k5cvk3) 2  [Intercept](#_fvuez67gvg0l) 2  [HTTP history](#_r77fxolg8fq8) 3  [**Modificar peticiones**](#_wkfvsnn2k2i1) **4**  [**Selección del objetivo**](#_l1cnup16eq1m) **5**  [Sala](#_j4ec4pi2aspx) 5  [Repetir solicitudes](#_8je6nqtij4bl) 7  [Historial](#_6f6lwfolhlgi) 9 |
| Instalación |
| <https://portswigger.net/burp/documentation/desktop/getting-started/download-and-install> |
| Interceptar peticiones |
| Proxy |
| Intercept |
|  |
|  |
| **Forward →** Continúa con la petición |
| Proxy > HTTP history |
|  |
| Lo que estamos viendo es el historial de peticiones HTTP. |
|  |
| Comparador de peticiónes y respuestas |
|  |
| Modificar peticiones |
| Proxy → Intercept |
| Url de ejemplo: |
| <https://portswigger.net/web-security/logic-flaws/examples/lab-logic-flaws-excessive-trust-in-client-side-controls> |
| Credenciales: |
| Nombre: **wiener**  Contraseña: **peter** |
|  |
| Podemos editar los datos del producto antes de enviarlos al carrito. |
| Selección del objetivo |
| **Sala** |
| <https://portswigger.net/web-security/information-disclosure/exploiting/lab-infoleak-in-error-messages> |
| Navegamos a la sala y seleccionamos la web |
| Proxy > HTTP history > //añadimos a la vista |
|  |
| Seleccionamos la barra de Filtros que se encuentra en la parte superior de los resultados y seleccionamos que se muestren solo los elementos en la vista. |
|  |
| Como resultado solo aparecerán las url contenido en nuestra vista |
|  |
| Repetir solicitudes |
| Cuando tenemos definida una url a estudiar, el módulo de **Repetidor** nos ayuda a enviar y editar la petición. |
|  |
|  |
|  |
| Pulsamos **send** y analizamos la respuesta. Podemos cambiar la información de la **request** antes de cada envío. |
|  |
| Historial |
|  |
| Envio de parámetros no esperados |
|  |
| Logramos un error en el servidor que nos deja ver información del error. |
|  |
| En este caso, con dicha información podemos encontrar vulnerabilidades |
|  |