

ANALISYS FORENSICS



Alumno:

Ahc0b

-2024-



INDICE

*CONTENIDO

1) <u>Introducción</u>	Pág. 3
2) <u>Objetivo</u>	Pág. 3
3) <u>Consigna</u>	Pág. 3
4) <u>Resolución</u>	Pág. 3
5) <u>Ingreso a Laboratorios</u>	Pág. 4
6) <u>Mis 5 Labs: Escenarios para Vulnerar</u>	Pág. 6
6.1) <u>LAB1: High-level logic vulnerability (APPRENTICE)</u>	Pág. 6
6.2) <u>LAB2: Low-level logic flaw (PRACTITIONER)</u>	Pág. 11
6.3) <u>LAB3: Inconsistent handling of exceptional input (PRACTITIONER)</u>	Pág. 16
6.4) <u>LAB4: Inconsistent security controls (APPRENTICE)</u>	Pág. 20
6.5) <u>LAB5: Password reset broken logic (APPRENTICE)</u>	Pág. 22
7) <u>Recomendaciones para Mitigación de Vulnerabilidades</u>	Pág. 27
8) <u>Conclusiones finales</u>	Pág. 28
9) <u>Fuentes</u>	Pág. 29



1) Introducción.



El alumno, tras haber completado el curso relacionado con el OWASP Top 10, con un enfoque en la identificación y mitigación de vulnerabilidades de seguridad en aplicaciones web, se prepara para aplicar los conocimientos adquiridos en la práctica. En esta etapa, el estudiante deberá elaborar un informe detallado sobre la temática elegida, demostrando su habilidad para identificar riesgos y aplicar las mejores prácticas de seguridad para proteger las aplicaciones. Este informe servirá como una prueba del entendimiento de los conceptos fundamentales del OWASP Top 10 y su capacidad para implementar soluciones efectivas.

2) Objetivo.



Analizar, procesar, aprender y demostrar su comprensión del OWASP Top 10 identificando riesgos en aplicaciones web y presentando un informe con soluciones adecuadas para mejorar la seguridad.

3) Consigna.



El docente procedió a dar la consigna para realizar, siendo los requisitos para poder obtener el certificado:

- Seleccionar 5 laboratorios de PORTSWIGGER o 5 laboratorios de DVWA.
- Realizarlos y documentar el paso a paso con capturas y desarrollo.
- Tiempo para realizarlo, 1 mes a partir del día de hoy (22/07/2024).

*****OBVIEDAD!:** no seleccionar los mismos que se hicieron en el curso.

4) Resolución.



En este caso se procedió a la realización de 5 laboratorios de PortSwigger. Esta es una empresa de ciberseguridad conocida principalmente por su herramienta de pruebas de penetración y análisis de seguridad web, **BurpSuite**.

Fundada en 2006, PortSwigger se especializa en proporcionar soluciones para detectar y abordar vulnerabilidades en aplicaciones web. BurpSuite es ampliamente utilizado por profesionales de la seguridad para realizar pruebas de seguridad en aplicaciones web, y la empresa también ofrece recursos educativos, investigaciones y publicaciones sobre ciberseguridad.

Dentro de su página web encontraremos diversas opciones en su menú, entre ellas la posibilidad de al crearte una cuenta realizar sus laboratorios para practicar con tres niveles de dificultades. Nosotros nos centraremos en 5 solamente y utilizaremos nuestra maquina Kali Linux para finalizarlos.

⊕ Link: <https://portswigger.net/>

 PortSwigger

LOGIN

Products ▾ | Solutions ▾ | Research | Academy | Support ▾ | ⌂

5) Ingreso a Laboratorios.

Nos dirigimos a <https://portswigger.net/>.

The screenshot shows the PortSwigger homepage. On the left, there's a large banner with the text "Trusted by security professionals." and a portrait of a man. On the right, a separate window titled "Burp Suite" is open, showing a list of "Sites" and a pie chart indicating "303" current issues. A red box highlights the "LOGIN" button at the top right of the main page.

Luego clic en “Login” nos realizamos una cuenta, es sencillo solo pide el email, luego recibes el correo con tu contraseña segura y sigues los pasos.

The screenshot shows the "Login" page. It has an orange header with the word "Login". Below it is a form with fields for "Email address" and "Password". There's a "Forgot your password?" link and a "Remember me on this computer" checkbox. At the bottom are two buttons: "Log in" (green) and "Create account" (grey). A red box highlights the "Create account" button.

Clic en “Crear Cuenta”, te recarga la página y solo completas la casilla con tu mail allí. Si todo es correcto te aparecerá el mensaje:

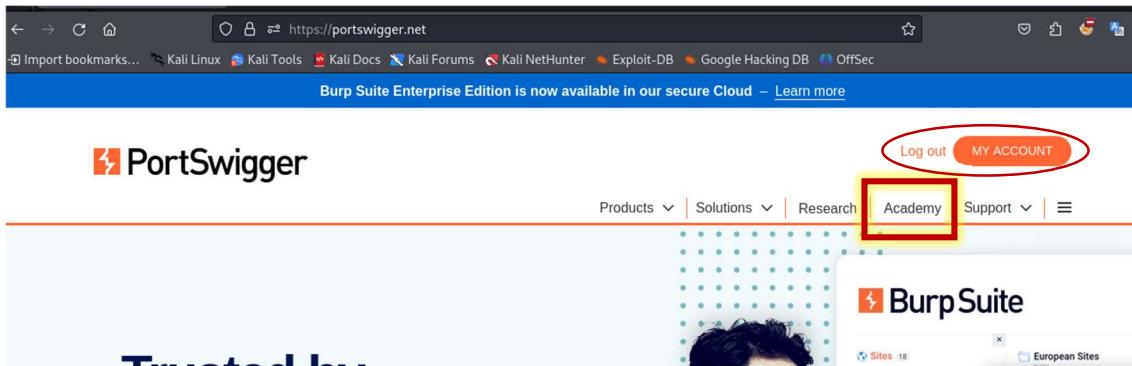
“Thank you. Please check your emails for instructions on how to complete your registration.”

The screenshot shows two side-by-side forms. On the left is the "Create your account" page with a field for "Email address" and a "Register" button. On the right is the "Register" page with a field for "Email address" and a "Register" button. Below the "Register" button is a message box containing the text "Thank you. Please check your emails for instructions on how to complete your registration." A red box highlights this message box.

Procedes entonces a entrar a tu email ver el correo que te han enviado para completar el registro y validar tu cuenta.

Una vez redirigido nuevamente a la página con la contraseña otorgada y tu email ya tienes tu cuenta para proceder a resolver los laboratorios.

Vemos que al ingresar ya nos aparece nuestra página de inicio con “My Account”, es decir estamos logueados.



Clic en la opción “Academy” que vemos en la imagen lado derecho superior y allí podemos ver si bajamos un poquito el acceso a los laboratorios. Clic en “VIEW ALL”.



Podemos ver los 3 niveles de dificultad de más fácil a más difícil, el orden seria:



This screenshot displays the "All labs" section of the PortSwigger Academy. It features a grid of lab challenges categorized by difficulty: *APPRENTICE, *PRACTITIONER, and *EXPERT. The challenges are organized into sections such as "Mystery lab challenge", "SQL injection", and "Reflected XSS". Each challenge card includes a "LAB" icon, the difficulty level, a brief description, and a status indicator like "Not solved". On the far right, there is a vertical banner with the "BURPSUITE" logo.

6) Mis 5 Labs: Escenarios para Vulnerar.

6.1) LAB1: High-level logic vulnerability (APPRENTICE).

Ingresamos al mismo.



Lab: High-level logic vulnerability



This lab doesn't adequately validate user input. You can exploit a logic flaw in its purchasing workflow to buy items for an unintended price. To solve the lab, buy a "Lightweight I33t leather jacket".

You can log in to your own account using the following credentials: `wiener:peter`

[ACCESS THE LAB](#)

Vemos que nos proporciona un usuario y contraseña (`wiener:peter`), además nos dice que el mismo no posee una validación de usuario, y que nuestra tarea es comprar con el dinero que tenemos allí o no en la cuenta, comprar el producto “Lightweight I33t leather jacket”. Procedemos a hacer clic en ACCESS THE LAB e ingresamos al laboratorio.

Vemos una página de e-commerce a simple vista podemos ver el producto de referencia a comprar. Procedemos entonces a utilizar nuestra herramienta BurpSuite y activamos el proxy.

Funcionando el mismo recargamos la página y pasamos a loguearnos (clic en "my account") con el usuario y contraseña dado (wiener:peter). Vemos que estamos adentro y tenemos \$100.00 solamente cuando el precio del producto para la resolución es de \$1337.00.

The screenshot shows two pages from the WebSecurity Academy lab. On the left is the 'Login' page, which has a 'Username' field containing 'wiener' and a 'Password' field containing '*****'. A 'Log in' button is at the bottom. On the right is the 'My Account' page, which displays the user's username 'wiener'. It also shows a 'Store credit: \$100.00' message, which is highlighted with a red box. Below this, there is a section for updating email.

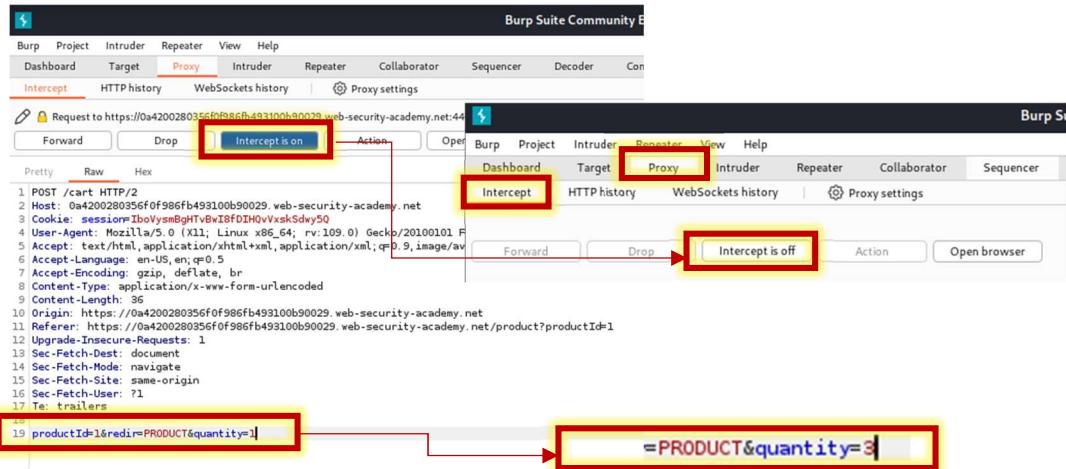
Procedemos entonces a sumarlo al carrito y tratar de mandar la orden de comprarlo a ver que sucede, luego analizaremos todas nuestras acciones en BurpSuite.

The screenshot shows a product page for a 'Lightweight "I33t" Leather Jacket'. The price is listed as '\$1337.00'. Below the price, there is a 'Quantity' input field set to '1', followed by an 'Add to cart' button, which is highlighted with a red box. To the right of the product image, there is a detailed description of the jacket.

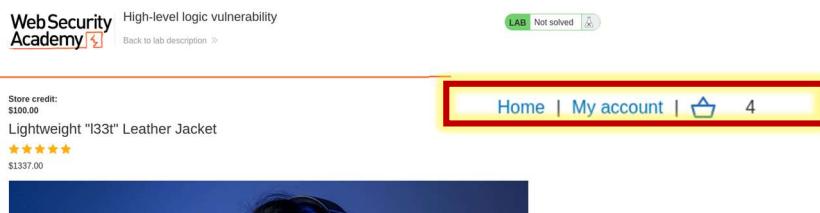
Agregamos al carrito clic en "Add to Cart" y luego vamos a comprarlo haciendo clic en "Place order". Observamos que nos dice arriba en rojo que no tenemos suficiente crédito para poder comprarlo. Procedemos entonces a ver nuestras solicitudes POST en nuestra herramienta.

The screenshot shows a 'Cart' page. At the top, there is a message 'Not enough store credit for this purchase' in a red box. Below this, there is a table with columns 'Name', 'Price', and 'Quantity'. One item in the cart is a 'Lightweight "I33t" Leather Jacket' priced at '\$1337.00'. There are buttons for quantity adjustment ('-', '+') and a 'Remove' button. Below the cart table, there is a 'Coupon:' input field with an 'Apply' button next to it. At the bottom, the total is shown as 'Total: \$1337.00' and there is a large 'Place order' button, which is highlighted with a red box.

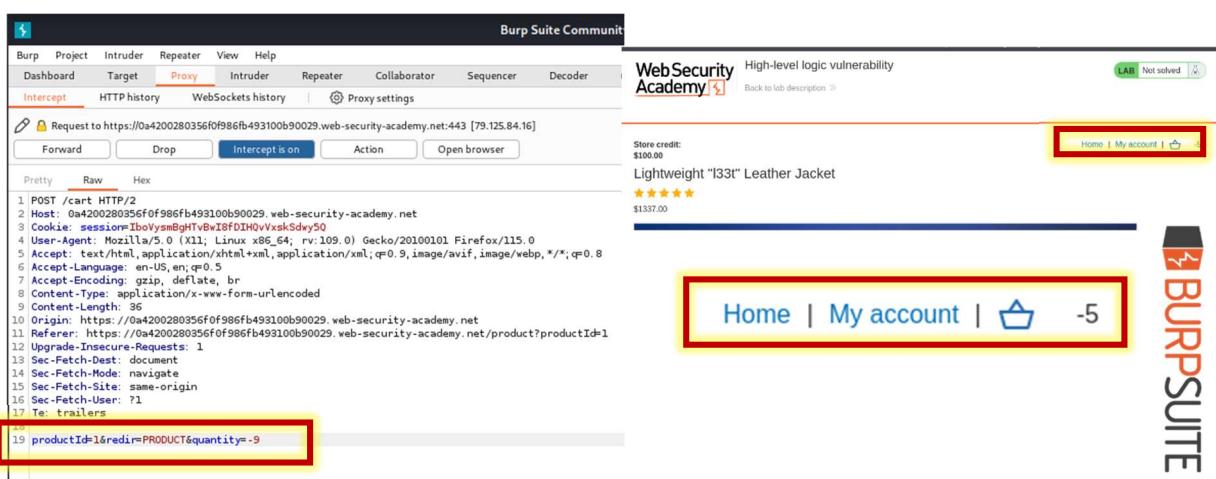
Vemos que en la solicitud POST de /cart no esta validada correctamente la cantidad en su peticion. Procedemos a interceptar la peticion cuando vamos a añadir al carrito un producto. Vamos en el Burp a "Intercept", y antes de hacer clic en "add to cart" en el producto clic en "intercept is off" para convertirlo en "intercept is on", automaticamente al dar clic en "add to cart" aparece nuestra ventana. Claramente previamente nuestro Proxy sigue encendido.



Es decir "quantity=1"esta presente como un numero el cual puede modificarse correctamente y no dentro de una variable, procedemos a modificarlo para ver si podemos agregar al carrito de 1 que ya teniamos a 3 mas, es decir 4 en total. Clic en forward para mandar la peticion, sacamos el "intercept is on" para convertirlo en "intercept is off" y actualizamos nuestra pagina. Efectivamente tenemos nuestros 4 productos.



Entonces que pasaria si repetimos el proceso, pero ahora si colocamos un numero negativo. Escribimos entonces "quantity=-9" ahora, forward y actualizamos la pagina vemos que si es correcto.



Observamos que admite precio negativo cuando ponemos cantidades negativas. Entonces realizamos la compra a ver si lo permite, pero vemos que sale el cartel en rojo que no admite valores en 0.

The screenshot shows a shopping cart with a single item: "Lightweight 'I33t' Leather Jacket" at \$1337.00. The quantity input field has a value of "-5". A red box highlights the error message "Cart total price cannot be less than zero" above the quantity input. Another red box highlights the total amount "-\$6685.00" below the input. The "Place order" button is visible at the bottom left.

Procedemos entonces a volver al principio sacamos el producto con "Remove" y añadimos solo nuestro producto a comprar como si lo haríamos realmente, y también los necesarios de precio más bajo al que queremos comprar para luego poniéndole cantidades negativas a dichos productos extras agregados nos resten el valor del producto realmente a comprar hasta llegar a un valor que se encuentre dentro del crédito que tenemos, y si es a un precio más bajo posible mejor. Vamos a la tienda entonces:

The screenshot shows a product listing page with four main items and two additional rows of items below. The items are:

- Lightweight "I33t" Leather Jacket**: \$1337.00 (highlighted with a red circle)
- Hologram Stand In**: \$90.41 (highlighted with a red circle)
- There's No Place Like Gnome**: \$30.15
- ZZZZZZ Bed - Your New Home Office**: \$2.41

Below these are two more rows of items:

- Cheshire Cat Grin**: \$16.75 (highlighted with a red circle)
- Real Life Photoshop**: \$4.59
- Adult Space Hopper**: \$99.08
- Portable Hat**: \$72.39

Each item has a "View details" button below it.

En mi caso entonces elegimos nuestro producto que es el primero, y también elijo el "Hologram Stand In" como también el "Cheshire Cat Grin".

Identificamos entonces nuestras peticiones POST en /cart en el Burp, cada una tendrá su “productold” y las mandamos ahora al Repeater de la siguiente manera haciendo clic derecho en la solicitud POST y luego “Send to Repeater”.

The screenshot shows the Burp Suite interface with a list of network requests. A right-click context menu is open over a POST request to '/cart'. The 'Send to Repeater' option is highlighted with a red box. The menu also includes other options like 'Send to Intruder', 'Send to Sequencer', 'Send to Comparer', etc.



Vamos en el menú a la sección del mismo y sacando la cuenta de nuestros productos elegidos para que lo podamos pagar lo más barato posible necesitaríamos -14 hologramas y -4 Cheshire Cat.

The screenshot shows the Burp Suite interface with a modified POST request to '/cart'. The 'productId=2&redir=PRODUCT&quantity=-14' parameter is highlighted with a yellow box. The modified request is then sent to the Repeater tab, which shows two product images with their respective quantities: '-14' and '-4'.

-14

-4

Mandamos con “Send” la petición cambiando la cantidad a -14, y luego repetimos el proceso con el otro producto mandándolo al repeater su solicitud POST y cambiando la cantidad a -4. Luego actualizamos la página y vamos al carrito y nos aparecerá lo siguiente:

The screenshot shows the website cart page. It lists three items: 'Lightweight "I33t" Leather Jacket', 'Hologram Stand In', and 'Cheshire Cat Grin'. The 'Hologram Stand In' and 'Cheshire Cat Grin' quantities are set to -14 and -4 respectively. The total price is \$4.26 and the 'Place order' button is visible.

La página no admite números negativos por lo que un precio se debe pagar, en nuestro caso compraríamos algo de \$1337.00 a solo \$4.26 utilizando el dinero crédito que tenemos, mandamos la orden para comprar “Place order”.

The screenshot shows a solved lab from the OWASP Web Security Academy. At the top, it says "Web Security Academy" and "High-level logic vulnerability". A green button indicates the task is "Solved". Below that, a yellow box highlights the message "Congratulations, you solved the lab!". To the right, there are links to "Share your skills!" and "Continue learning >". The main content area displays the order details: "Your order is on its way!" followed by a table of items and their prices. A large green checkmark icon is on the right. At the bottom left, a yellow box highlights the total price: "Total: \$4.26". A green button at the bottom right also says "LAB Solved".

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$1337.00	1
Hologram Stand In	\$90.41	-14
Cheshire Cat Grin	\$16.75	-4

Finalmente hemos realizado la compra de “Lightweight I33t leather jacket”, el laboratorio se resolvió satisfactoriamente.

6.2) LAB2: Low-level logic flaw (PRACTITIONER).

Pasamos a una continuación del anterior laboratorio el objetivo es comprar nuevamente el mismo producto “Lightweight I33t leather jacket”, mismo login pero esta vez posee una vulnerabilidad de validación de usuario con respecto a la cantidad máxima de productos con la que está programado este mercado.

The screenshot shows the "Low-level logic flaw" lab page. It has tabs for "LAB" (selected), "PRACTITIONER" (highlighted in blue), and "Not solved". Below the tabs, there's a brief description of the challenge: "This lab doesn't adequately validate user input. You can exploit a logic flaw in its purchasing workflow to buy items for an unintended price. To solve the lab, buy a "Lightweight I33t leather jacket".

Lab: Low-level logic flaw

The screenshot shows the "My Account" section. On the left is a "Login" form with fields for "Username" (wiener) and "Password" (*****). On the right, the "Store credit:" field is highlighted with a red box and contains the value "\$100.00". Below the account section, a message says "Your username is: wiener".

Procedemos entonces a loguearnos, vemos la cuenta wiener con los \$100 de crédito.

The screenshot shows the "My Account" section. On the left is a "Login" form with fields for "Username" (wiener) and "Password" (*****). On the right, the "Store credit:" field is highlighted with a red box and contains the value "\$100.00". Below the account section, a message says "Your username is: wiener".

Con el Burp activado como vimos en LAB1 agregamos al carrito nuestro producto y luego vamos a dicho programa a ver las solicitudes POST /cart.



Allí encontramos nuestra solicitud. Modificamos el ultimo parámetro “quantity=99”, siendo el ultimo numero de 2 dígitos posible para que nos acepte la petición, si es mayor nos dará error. Luego cambiado el numero por 99 mandamos la solicitud al Intruder.

Así se verá en el Intruder, procedemos ir a Payloads y colocaremos las siguientes características de imagen; Payload type=NULL Payloads y en Payloads Settings tildamos la opción= Continue Indefinitely. Luego clic en Start attack.

Se procede entonces a comenzar con el ataque donde automáticamente y de manera indefinida se mandan peticiones POST agregando el artículo seleccionado al carrito.



11. Intruder attack of https://0a8f00fb03868517824e25ef009500c2.web-security-academy.net

Results	Positions	Payloads	Resource pool	Settings		
Filter: Showing all items						
Request	Payload	Status code	Error	Timeout	Length	Comment
0	null	302	<input type="checkbox"/>	<input type="checkbox"/>	100	
1	null	302	<input type="checkbox"/>	<input type="checkbox"/>	100	
2	null	302	<input type="checkbox"/>	<input type="checkbox"/>	100	
3	null	302	<input type="checkbox"/>	<input type="checkbox"/>	100	
4	null	302	<input type="checkbox"/>	<input type="checkbox"/>	100	
5	null	302	<input type="checkbox"/>	<input type="checkbox"/>	100	
6	null	302	<input type="checkbox"/>	<input type="checkbox"/>	100	



Lo dejamos correr y actualizamos nuestro carrito veremos que se van modificando nuestra cantidad en el carrito, llegado a una cantidad en la que el precio se vuelve negativo. Allí hemos vulnerado el sistema llegando a su cantidad máxima programada y comienza una cuenta regresiva.

The screenshot shows a shopping cart interface with two states. On the left, a 'Cart' section shows a single item: 'Lightweight "I33t" Leather Jacket' with a price of '\$1337.00' and a quantity of '5049'. A red box highlights the '\$100.00' store credit. Below it is a 'Quantity' input field with a minus sign and a plus sign. A red circle highlights the quantity value. A 'Remove' button is also visible. On the right, the same item is shown with a quantity of '16137'. A black box labeled 'AUMENTO' is placed above the quantity input field. A red circle highlights the quantity value. Below both sections is a 'Coupon' input field with 'Add coupon' and 'Apply' buttons. The total price is shown as 'Total: \$6750513.00' on the left and 'Total: -\$21374503.96' on the right. Red arrows point from the 'AUMENTO' box to the quantity input field and from the 'DISMINUYE' box to the total price on the right.

Vemos que el precio bajo, pero lo que haremos es que seguiremos mandando peticiones por medio del Intruder pero configurandolo de una manera de controlar la cantidad de productos que se van a agregar. En este momento la cantidad va a seguir aumentando en nuestro carrito pero el precio es quien disminuirá al mandar las peticiones. Utilizamos de nuevo nuestra petición POST con la cantidad 99 pero en el intruder configuraremos lo siguiente:

The screenshot shows the Burp Suite Intruder tool configuration. At the top, the 'Intruder' tab is selected. In the 'Payload sets' section, a payload set of '1' is selected with a payload count of '323' and a payload type of 'Null payloads'. In the 'Request headers' section, there are checkboxes for 'Update Content-Length header' and 'Set Connection header'. In the 'Error handling' section, there are fields for 'Number of retries on network failure' (set to 1) and 'Pause before retry (milliseconds)' (set to 2000). A yellow box highlights the payload settings and error handling sections.

Damos a Start attack y vemos que empieza a hacer las peticiones, si actualizamos nuestro mercado veremos que empieza el fenómeno nombrado.

The screenshot shows the 'Results' tab of the OWASP ZAP Intruder tool. It displays a table of requests with columns for Request, Payload, Status code, Error, Timeout, Length, and Comment. The status codes for all four requests are 302. Below the table is a progress bar indicating 72 of 323 requests have been processed.

Se hicieron la cantidad de peticiones necesarias, al cumplirse ya teníamos un numero al cual era mas fácil sacar una cuenta para dejar el precio entre \$1 y \$100. Nos había quedado un precio de -\$64.060,96 que dividido el precio del producto es decir \$1.337,00 nos da una cantidad para el Repeater de 47,91.

The screenshot shows a web store interface. In the cart section, a product named "Lightweight 'I33t' Leather Jacket" is listed with a price of \$1337.00. The quantity input field contains the value 32076, which is highlighted with a red circle. Below the cart, a message indicates a total credit of \$100.00. At the bottom, a yellow box highlights the total price of -\$64060.96.

Por ende, ahora mandamos la solicitud POST al Repeater y agregamos 47 del producto principal.

The screenshot shows the Burp Suite Repeater tool. A POST request is being sent to the endpoint /cart HTTP/2. The request parameters include productId=1, redir=PRODUCT, and quantity=47. The response shows a 302 Found status with a Location header pointing to /product?productId=1. A red box highlights both the request parameters and the response status.

Como resultado vemos que solo quedan -\$1221,96.

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$1337.00	32123

Coupon:
Add coupon
Apply

Total: -\$1221.96

Como no podemos agregar un producto mas del mismo, agregamos otro producto cualquiera de la tienda para que siendo positivo disminuya el precio hasta llegar a un precio positivo menor a \$100.

Sabiendo el precio del producto saco la cantidad necesaria para llegar al precio, en nuestro caso 22 Mood Enhacer.

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$1337.00	32123
Mood Enhancer	\$56.86	22

Coupon:
Add coupon
Apply

Total: \$28.96

Place order

Nuestro precio por TODOS estos artículos es de \$28,96 dentro de nuestro crédito, procedemos a comprarlo.

Congratulations, you solved the lab!

Share your skills! Continue learning >

Store credit:
\$71.04

[Home](#) | [My account](#) | 0

Your order is on its way!

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$1337.00	32123
Mood Enhancer	\$56.86	22

Total: \$28.96



LAB Solved



6.3) LAB3: Inconsistent handling of exceptional input (PRACTITIONER).

En este LAB hay un problema de validacion de usuario en el proceso de registro, que permite al atacante poder ingesar como usuario administrativo y acceder a privilegios. En esta oportunidad tendriamos que acceder al panel de administracion y borrar el usuario llamado Carlos.



Lab: Inconsistent handling of exceptional input



This lab doesn't adequately validate user input. You can exploit a logic flaw in its account registration process to gain access to administrative functionality. To solve the lab, access the admin panel and delete the user `carlos`.

Con el Burp funcionando accedemos al laboratorio vemos que es un e-commerce que nos deja registrarnos. Vemos que nos permite tener un mail dentro de la pagina en su parte superior realizamos clic allí.

Tenemos nuestra casilla de mails.

Inbox is empty

Pasamos a registrarnos y ya nos proporciona informacion adicional sobre como tener privilegios únicos como usuario, allí se observa que se obtiene privilegios solo usuarios terminados en @dontwannacry.com.

Register

If you work for DontWannaCry, please use your @dontwannacry.com email address

Probamos creando una cuenta normalmente. Revisamos el mail y confirmamos la solicitud para ser un usuario valido.

Register

If you work for DontWannaCry, please use your @dontwannacry.com email address

Your email address is attacker@exploit-0a5100db03c2077382318dc4012200be.exploit-server.net

Displaying all emails (@exploit-0a5100db03c2077382318dc4012200be.exploit-server.net and all subdomains)

Subject	Body
attacker.user1@exploit-0a5100db03c2077382318dc4012200be.exploit-server.net no-reply@0a860006c032d077d Account registration	Hello! Please follow the link below to confirm you https://0a860006c032d077d@02658ee700df0030.web-security-academy.net Thanks, Support team



Inconsistent handling of exceptional input

[Back to lab home](#)

[Email client](#)

[Back to lab description >](#)

Clic en el enlace para validación.

Account registration successful!

[Home](#) | [My account](#) | [Register](#)

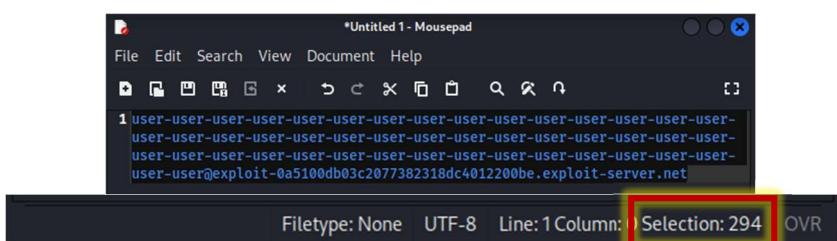
Entramos a la cuenta y no vemos nada raro en si solo que podemos agregar cualquier nombre y poner @exploit-0a5100db03c2077382318dc4012200be.exploit-server.net y nos llegar a nuestro correo. Si nos logueamos vemos lo siguiente;

My Account

Your username is: user1

Your email is: attacker.user1@exploit-0a5100db03c2077382318dc4012200be.exploit-server.net

Sabiendo esto, procederemos a chequear si tiene una cantidad máxima de caracteres para nuestro email. Abrimos un blog de notas y creamos un nombre de usuario largo en nuestro caso intentamos con uno de 294 caracteres.



Nos registramos nuevamente con dicho correo y validamos.

Register

If you work for DontWannaCry, please use your @dontwannacry.com email address

Your email address is attacker@exploit-0a5100db03c2077382318dc4012200be.exploit-server.net

Displaying all emails (@exploit-0a5100db03c2077382318dc4012200be.exploit-server.net and all subdomains)

Subject	Body
user-user-user-user@exploit-0a5100db03c2077382318dc4012200be.exploit-server.net no-reply@0a860006c032d077d Account registration	Hello! We're happy to confirm your email and complete registration. https://0a860006c032d077d@02658ee700df0030.web-security-academy.net Thanks, Support team

Web Security Academy | Inconsistent handling of exceptional input

LAB Not solved

[Home](#) | [My account](#) | [Register](#)

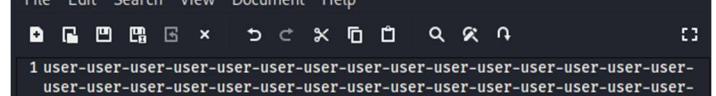
Clic en el enlace para validación.

Entramos a la cuenta en cuestión logueandonos.

My Account

Your username is: user2

Notamos que el email no está completo ya que era (user-user@exploit-0a5100db03c2077382318dc4012200be.exploit-server.net), falta dicha parte sombreada en amarillo, por lo que procedemos a colocarlo en el blog de notas para saber cuántos caracteres acepta.



The screenshot shows a terminal window titled "Untitled 1 - Mousepad". The menu bar includes File, Edit, Search, View, Document, Help, and a set of icons. The toolbar below has icons for file operations like Open, Save, Print, and a search bar. The main text area contains three lines of a password dump:

```
1 user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user@exploit-0a5100db03c2077382318dc4012200be.exploit-server.net
2
3 user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-user@exploit-0a5100db03c2
```

The bottom status bar shows "Filetype: None", "UTF-8", "Line: 3 Column: 0", "Selection: 255", and "OVR". A red box highlights the status bar.

Vemos que acepta hasta 255. Lo que se procede entonces es crear un último usuario el cual esté vinculado a nuestro email y también pueda tener privilegios. Para esto lo que se hace es un correo que justo en el carácter 255 termine con el dominio @dontwannacry.com, luego separarla por un punto y relacionarlo con nuestro email para que nos llegue la validación. Quedando de la siguiente manera:

```
5  
6 ser-user-user-user-user-user-user-user-user-user-user-user-user-user-  
user-user-user-user-user-user-user-user-user-user-user-user-user-user-  
user-user-user-user-user-user-user-user-user-user-user-user-user-user-  
user-user-  
user@dontwannacry.com.exploit-0a5100db03c2077382318dc4012200be.exploit-  
server.net|
```

Nos queda un mail extenso, pero observamos que el carácter 255 cortaría dicho mail al ingresar en la cuenta creada. Hacemos coincidir con la ultima "m" de @dontwannacry.com dicho número de carácter.

```
6  
7 ser-user-user-user-user-user-user-user-user-user-user-user-user-user-user-  
user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-  
user-user-user-user-user-user-user-user-user-user-user-user-user-user-user-  
user-user-  
user@dontwannacry.com.exploit-0a5100db03c2077382318dc4012200be.exploit-  
server.net
```

Seguimos registrando un nuevo usuario y validando.

Register

If you work for DontWannaCry, please use your @dontwannacry.com email address

Username	user10
Email	@user@dontwannacry.com.exploit-0a5100db03c2077382318dc4012200be.exploit-server.net
Password	*****
<input type="button" value="Register"/> 	

Your email address is attacker@exploit-0a5100db03c2077382318dc4012200be.exploit-server.net

Displaying all emails (Message ID:1000005c2077382318dc4012200be.exploit-server.net and subject:)

Sent

To

RE: Account registration

From: reply@0a5100db03c2077382318dc4012200be.exploit-server.net
Date: 2024-07-29 19:53:57 +0000
Subject: RE: Account registration
To: attacker@exploit-0a5100db03c2077382318dc4012200be.exploit-server.net
Message-ID: 32c077d969e659eebe780f0030.web-security-academy.net
Content-Type: multipart/related; boundary="001urPnHg5o0wP50r79v0q"

Clic en el enlace para validación.

NETCAT

Please follow the link below to complete your registration.

<https://0a5100db03c2077382318dc4012200be.exploit-server.net/account/registration/659eebe780f0030.web-security-academy.net/registration-token/001urPnHg5o0wP50r79v0q>

Support team

Nos logueamos y allí vemos que definitivamente nos cortó el email y parecemos tener un mail de administrador

Home | Admin panel | My account | Log out

My Account

Your username is: user10

Your email is: ser-user@dontwannacry.com

Vamos a la opción nueva que nos aparece "Admin panel".

Home | Admin panel | My account | Log out

Allí encontramos a todos los usuarios, hasta los propios creados, y en especial a nuestro amigo el usuario Carlos. Clic en Delete para eliminarlo.

Users

carlos - Delete

Logramos resolver el laboratorio.



Inconsistent handling of exceptional input

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home | Admin panel | My account

Users

wiener - Delete
user1 - Delete
user2 - Delete
user10 - Delete

LAB Solved



6.4) LAB4: Inconsistent security controls (APPRENTICE)

En este caso es una version del problema anterior con a una interaccion con el server interno para actualizar nuestro mail una vez registrados. No existe una validacion de usuario por lo que lograr tener el usuario admin es mas facil de lo que se piensa.

This lab's flawed logic allows arbitrary users to access administrative functionality that should only be available to company employees. To solve the lab, access the admin panel and delete the user carlos.

Entramos al laboratorio, igual que el anterior es un ecommerce, tenemos nuestro email server y procedemos al registro de un usuario y la validación.

If you work for DontWannaCry, please use your @dontwannacry.com email address

Username: user1
Email: iddddd@dontwannacry.com.exploit-0ad9009a04fe91f982b95393011400ae.exploit-server.net
Password:
Register

Sent: 2024-07-29 20:10:56 To: dddddd@dontwannacry.com.exploit-0ad9009a04fe91f982b95393011400ae.exploit-server.net From: 404b61c3827205 49600810ea.we Subject: Hello! Body: Please follow the link below to confirm your email and complete registration.

Accord: https://8aa509de4bb91e38... View raw
Registration: https://academy.net/register?token=6h72K5C133NL4BALMjJ0220V
@gyTSA

Thanks,
Support team

Clic en el enlace para validación.

Nos logueamos y accedemos a nuestra cuenta.

My Account

Your username is: user1
Your email is: dddddd@dontwannacry.com.exploit-0ad9009a04fe91f982b95393011400ae.exploit-server.net

Email:
Update email

Vemos allí que nos da la opción de actualizar nuestro mail. Procedemos a hacer terminar en el dominio de administrador (quiero-usuario)@dontwannacry.com

My Account

Your username is: user1
Your email is: dddddd@dontwannacry.com.exploit-0ad9009a04fe91f982b95393011400ae.exploit-server.net

Email: idddd@dontwannacry.com
Update email

Actualizamos el email y ocurre lo siguiente:

Web Security Academy  Inconsistent security controls

[Email client](#) [Back to lab description >](#)

[Home](#) | [Admin panel](#) | [My account](#) | [Log out](#)

Ya nos aparece el “Admin panel”, no existe una validación mediante el server o email, ya solo siendo usuario puedes ponerte el email que desees.



Entramos al panel y borramos entonces a Carlos.

Users

wiener - Delete
carlos - Delete
user1 - Delete

Resolvimos nuestro laboratorio.

WebSecurity Academy  Inconsistent security controls

Back to lab description »

LAB Solved 

Congratulations, you solved the lab!

Share your skills!   Continue learning »

User deleted successfully!

Users

wiener - Delete

user1 - Delete

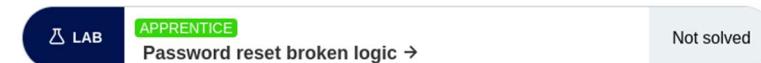


LAB Solved 

Home | Admin panel | My account

6.4) LAB5: Password reset broken logic (APPRENTICE)

En dicho LAB corresponde a una vulnerabilidad de funcionalidad cuando queremos recuperar nuestra contraseña, si interceptamos nuestra petición POST comprobamos que no está validado el token de sesión por lo que podemos modificar datos y mandar la petición para entrar a un usuario. En este caso el usuario a entrar se llama Carlos y nos da las credenciales de usuario conocido anteriormente (wiener:peter).



Lab: Password reset broken logic



This lab's password reset functionality is vulnerable. To solve the lab, reset Carlos's password then log in and access his "My account" page.

- Your credentials: wiener:peter
- Victim's username: carlos

Con el Burp funcionando y el proxy encendido, entramos a nuestro LAB. Vemos que tenemos un servicio de email y que es un blog, procedemos aloguearnos.

The screenshot shows the 'Web Security Academy' interface with the 'Password reset broken logic' lab selected. The 'Email client' button is highlighted with a red box. The 'My account' link in the navigation bar is also highlighted with a red box.

Login

Username: wiener
Password:

[Forgot password?](#)

My Account

Your username is: wiener
Your email is: wiener@exploit-0a4b00b1044908fc84c017dd0182005a.exploit-server.net

Email

Ya logueados vemos que tenemos nuestro email y somos el usuario weiner, abrimos nuestra casilla de email y cerramos nuestra sesión.

The screenshot shows the 'Web Security Academy' interface with the 'My account' page selected. A message at the top states 'Your email address is wiener@exploit-0a4b00b1044908fc84c017dd0182005a.exploit-server.net'. The 'Log out' link in the navigation bar is highlighted with a yellow box.

Vamos al panel de Login y procedemos a hacer clic en “Forgot password?” allí luego nos pedirá nuestro email o usuario, simulamos como que queremos recuperar nuestra contraseña y la hemos perdido. (Submit)

Enseguida llega el email, clic en enlace y colocamos nuestra nueva contraseña.



Visitamos entonces nuestro BURPSUITE para ver nuestras peticiones POST, en especial la de recuperación de contraseña /forgot-password?temp-forgot-password. La mandamos al Repeater clic derecho y “Send to Repeater”.

Vemos allí que posee en la parte superior un token de la password, procedemos a eliminarlo y mandar nuevamente la petición para ver si interactúa con la base de datos o nos da error.

Borrado dicho token como se denota ahí, mandamos la petición. Al parecer vemos que nos da Correcto.

The screenshot shows the Burp Suite interface with the Repeater tab selected. The Request pane contains a POST request to `/forgot-password?temp-forgot-password-token=...`. The Response pane shows a 200 OK response with the following headers and body:

```

HTTP/2 200 OK
Location: /
X-Frame-Options: SAMEORIGIN
Content-Length: 0

```

Probamos loguearnos nuevamente y todo sigue igual, se mandó la petición correctamente de cambio de contraseña. Comprobado, cerramos la sesión.

Login

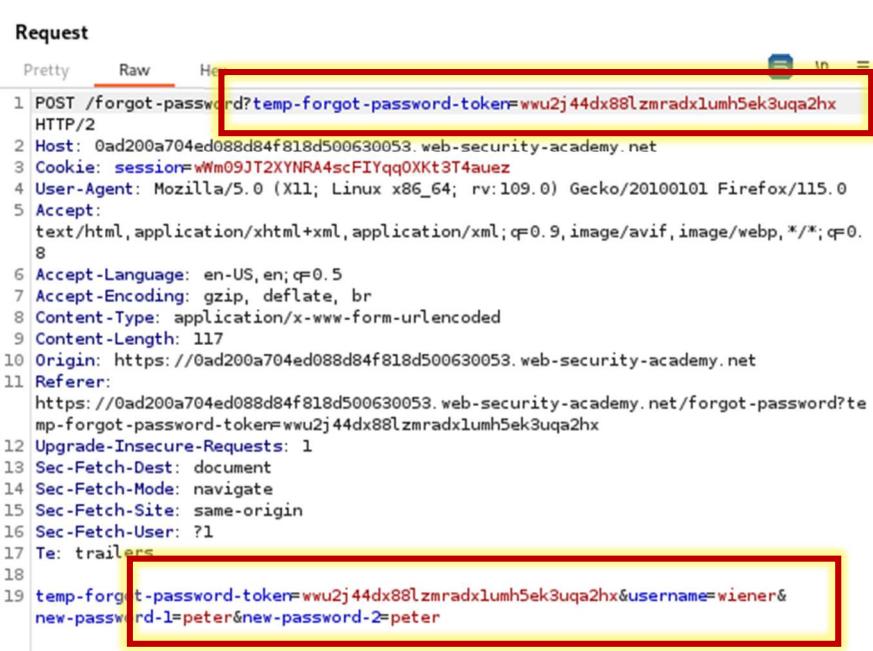
The screenshot shows a login page and a My Account page. On the left, the login form has 'wiener' in the Username field and the 'Log in' button highlighted. On the right, the My Account page shows 'wiener' as the username and includes a 'Log out' button.

Procedemos de nuevo entonces a repetir los pasos, vamos a login clic en "Forgot password?", ponemos nuestro usuario, vamos al mail validamos nueva contraseña y por ultimo vamos a la petición POST en /forgot-password?temp-forgot-password y la mandamos al Repeater.

Login

The screenshot shows the Burp Suite Repeater tool. A red arrow points to the 'Send to Repeater' option in the context menu for the last POST request. The repeater list shows several requests, including a POST to /forgot-password?temp-forgot-password. The context menu also includes 'Add to scope', 'Scan', 'Send to Intruder', 'Send to Sequencer', and 'Send to Organizer'.

Esta es nuestra petición al el Repeater.



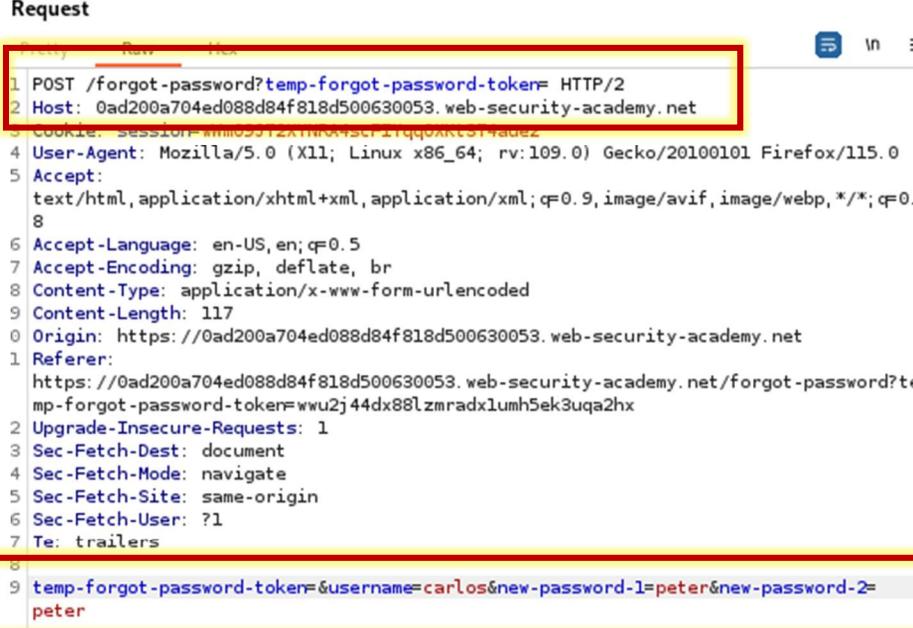
```

Request
Pretty Raw He
1 POST /forgot-password?temp-forgot-password-token=wwu2j44dx88lzmradxlumh5ek3uqa2hx
HTTP/2
2 Host: 0ad200a704ed088d84f818d500630053. web-security-academy.net
3 Cookie: session=wMm09JT2XYNRA4scFIYqq0XKt3T4auez
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 117
10 Origin: https://0ad200a704ed088d84f818d500630053. web-security-academy.net
11 Referer:
https://0ad200a704ed088d84f818d500630053. web-security-academy.net/forgot-password?te
mp-forgot-password-token=wwu2j44dx88lzmradxlumh5ek3uqa2hx
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18
19 temp-forgot-password-token=wwu2j44dx88lzmradxlumh5ek3uqa2hx&username=wiener&
new-password-1=peter&new-password-2=peter

```



Pasaremos a borrar los tokens arriba y abajo dejándolos vacíos en la petición que hemos marcado y modificaremos el username al usuario que conocemos y queremos entrar siendo “carlos”. Si la petición es tomada automáticamente cambiara la contraseña de carlos, siendo la nueva contraseña “peter” de este usuario. Quedara de la siguiente manera:



```

Request
Pretty Raw He
1 POST /forgot-password?temp-forgot-password-token=
HTTP/2
2 Host: 0ad200a704ed088d84f818d500630053. web-security-academy.net
3 Cookie: session=wMm09JT2XYNRA4scFIYqq0XKt3T4auez
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 117
0 Origin: https://0ad200a704ed088d84f818d500630053. web-security-academy.net
1 Referer:
https://0ad200a704ed088d84f818d500630053. web-security-academy.net/forgot-password?te
mp-forgot-password-token=wwu2j44dx88lzmradxlumh5ek3uqa2hx
2 Upgrade-Insecure-Requests: 1
3 Sec-Fetch-Dest: document
4 Sec-Fetch-Mode: navigate
5 Sec-Fetch-Site: same-origin
6 Sec-Fetch-User: ?1
7 Te: trailers
8
9 temp-forgot-password-token=&username=carlos&new-password-1=peter&new-password-2=
peter

```



Cabe aclarar que nosotros decidimos ponerle la misma contraseña que tenía el usuario wiener, podría haberse puesto cualquier otra. Procedemos a mandar la petición entonces una vez configurado correctamente todo.

```

Request
Pretty Raw Hex
1 POST /forgot-password?temp-forgot-password-token= HTTP/2
2 Host: 0ad200a704ed088d84f818d500630053.web-security-academy.net
3 Cookie: session=wMm09J2XYNRA4scFIYqqOXKt3T4auz
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 85
10 Origin: https://0ad200a704ed088d84f818d500630053.web-security-academy.net
11 Referer: https://0ad200a704ed088d84f818d500630053.web-security-academy.net/forgot-password?temp-forgot-password-token=www2j44dx88lzmradxlumh5ek3uqa2hx
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18
19 temp-forgot-password-token=&username=carlos&new-password-1=peter&new-password-2=peter
  
```

BURPSUITE

Vemos que la solicitud se ha mandado por lo que procedemos a loguearnos como un tal carlos y nuestra contraseña.

Login

Username: carlos
Password: [REDACTED]

[Forgot password?](#)

Log in



Password reset broken logic

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: carlos

Your email is: carlos@carlos-montoya.net

Email: [REDACTED]

Update email



Definitivamente somos el usuario Carlos y estamos en su cuenta.

LAB Solved

7) Recomendaciones para Mitigación de Vulnerabilidades.



LAB1: High-level logic vulnerability (APPRENTICE)

Para mitigar las vulnerabilidades de alto nivel en la lógica de la aplicación:

- Validación de Flujos de Trabajo: Implementa controles rigurosos para validar los flujos de trabajo y asegurarte de que todas las transiciones y estados se comporten como se espera.
- Pruebas Exhaustivas: Realiza pruebas exhaustivas de los escenarios de flujo de trabajo para identificar y corregir problemas en la lógica de la aplicación.
- Revisión de Código: Establece procesos de revisión de código regular para identificar y corregir errores lógicos antes de que lleguen a producción.
- Segregación de Roles y Responsabilidades: Asegúrate de que las responsabilidades y permisos estén claramente definidos y segregados para evitar accesos indebidos o acciones incorrectas.

LAB2: Low-level logic flaw (PRACTITIONER)

Para abordar fallos lógicos de bajo nivel:

- Validación de Entrada: Asegúrate de que todas las entradas sean validadas rigurosamente y que se manejen adecuadamente los datos inesperados.
- Manejo de Errores: Implementa un manejo de errores robusto para detectar y gestionar errores de manera segura, evitando la divulgación de información sensible.
- Pruebas Unitarias: Desarrolla y ejecuta pruebas unitarias que cubran posibles escenarios de fallo para identificar y corregir defectos lógicos.
- Auditoría de Código: Realiza auditorías de código enfocadas en lógica para encontrar y remediar defectos en la implementación.

LAB3: Inconsistent handling of exceptional input (PRACTITIONER)

Para manejar de manera consistente las entradas excepcionales:

- Estándares de Manejo de Excepciones: Define y aplica estándares uniformes para el manejo de excepciones y entradas inválidas en toda la aplicación.
- Validación y Sanitización: Valida y sanitiza todas las entradas de usuarios para evitar que datos maliciosos o inesperados afecten el sistema.
- Monitoreo y Registro: Implementa un sistema de monitoreo y registro para capturar y analizar excepciones, identificando patrones que podrían indicar problemas subyacentes.
- Manejo Centralizado de Errores: Utiliza un sistema centralizado para el manejo de errores que garantice un tratamiento uniforme y seguro de las excepciones.



LAB4: Inconsistent security controls (APPRENTICE)

Para evitar controles de seguridad inconsistentes:

- Implementación de Políticas de Seguridad: Establece y aplica políticas de seguridad uniformes a lo largo de toda la aplicación, asegurando consistencia en su implementación.
- Revisión de Configuración: Realiza revisiones periódicas de las configuraciones de seguridad para garantizar que todos los controles estén correctamente aplicados y actualizados.
- Automatización de Controles: Utiliza herramientas de automatización para aplicar y verificar controles de seguridad de manera consistente.
- Capacitación Continua: Capacita a los desarrolladores y administradores sobre la importancia de la seguridad y cómo aplicar controles de manera consistente.



LAB5: Password reset broken logic (APPRENTICE)

Para solucionar problemas en la lógica de reseteo de contraseñas:

- Proceso de Verificación: Implementa un proceso de verificación robusto para la autenticidad del usuario antes de permitir el restablecimiento de la contraseña.
- Enlaces Temporales: Utiliza enlaces temporales para la reactivación de contraseñas, asegúrandote de que expiren después de un corto período de tiempo para minimizar el riesgo de abuso.
- Registro de Eventos: Mantén registros detallados de los eventos de restablecimiento de contraseñas para poder auditar y responder a actividades sospechosas.
- Pruebas de Seguridad: Realiza pruebas de seguridad enfocadas en el proceso de restablecimiento de contraseñas para identificar y corregir cualquier debilidad en la lógica.

8) Conclusión final.

En conclusión, los laboratorios realizados con BurpSuite han demostrado la eficacia de herramientas como Intruder y Repeater en la identificación y análisis de vulnerabilidades web. A través de estos laboratorios, hemos descubierto diversas debilidades en la lógica de las aplicaciones y el manejo de excepciones, resaltando la importancia crítica de una configuración adecuada y segura.

Las vulnerabilidades identificadas podrían ser explotadas para causar daños significativos, subrayando la necesidad de aplicar rigurosas medidas de seguridad para proteger la integridad y confidencialidad de las aplicaciones web. Una forma correcta de mitigar estos errores es realizar las pruebas y control junto con políticas de privacidad para garantizar la confidencialidad del usuario.



6) Fuentes

- Apuntes de clases – ARPAC IT – OWASP 
- Pagina Oficial PortSwigger: <https://portswigger.net/>.



 **PortSwigger** 

 **BURPSUITE**