Business logic vulnerabilites

Lab 1: Excessive trust in client-side controls

**APPRENTICE**

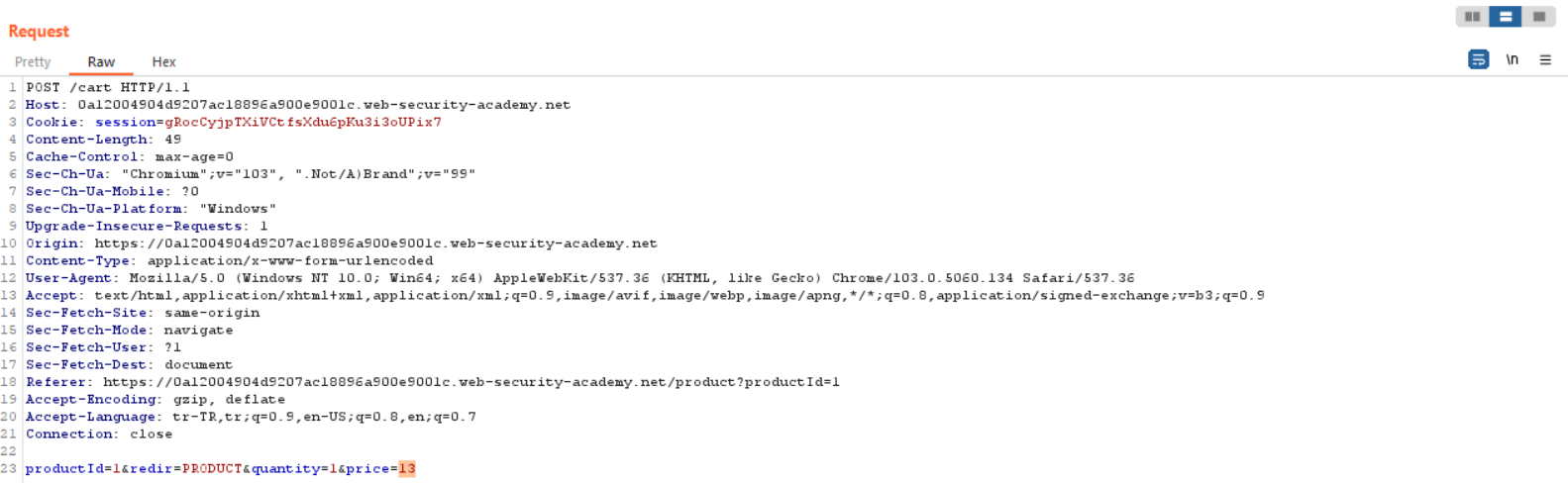
This lab doesn't adequately validate user input. You can exploit a logic flaw in its purchasing workflow to buy items for an unintended price. To solve the lab, buy a "Lightweight l33t leather jacket".

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

[**Access the lab**](https://portswigger.net/academy/labs/launch/ca187b1fb490deddce4034d443cb9afbf5b8279422a765b7d48040c50f327e9b?referrer=%2fweb-security%2flogic-flaws%2fexamples%2flab-logic-flaws-excessive-trust-in-client-side-controls)

**Solution**

1. With Burp running, log in and attempt to buy the leather jacket. The order is rejected because you don't have enough store credit.
2. In Burp, go to "Proxy" > "HTTP history" and study the order process. Notice that when you add an item to your cart, the corresponding request contains a price parameter. Send the POST /cart request to Burp Repeater.
3. In Burp Repeater, change the price to an arbitrary integer and send the request. Refresh the cart and confirm that the price has changed based on your input.
4. Repeat this process to set the price to any amount less than your available store credit.
5. Complete the order to solve the lab.



Add to cart requestindeki price kısmını değiştirebiliyorsun, zafiyet bu, pahalı olan ürünün fiyatını azaltıp ürünü alma olayı

Alacağımızı ürünün fiyatını, başka bir ürünü – miktar ekleyerek, fiyatı düşürme olayı.

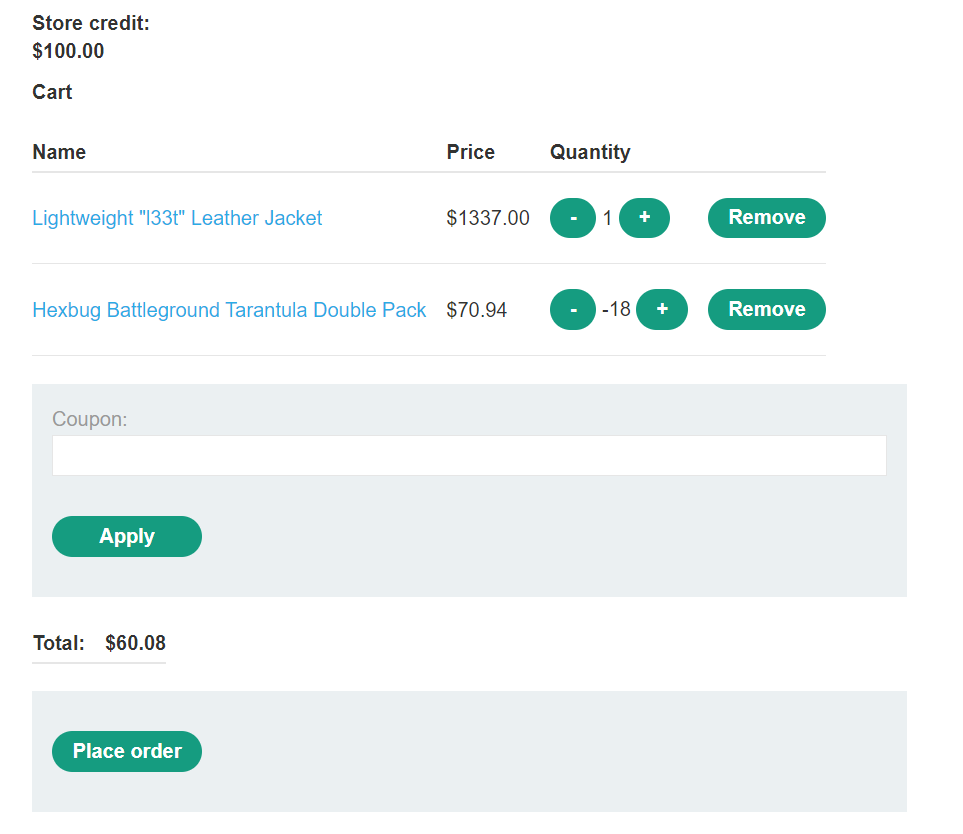
Lab 2: High-level logic vulnerability

**APPRENTICE**

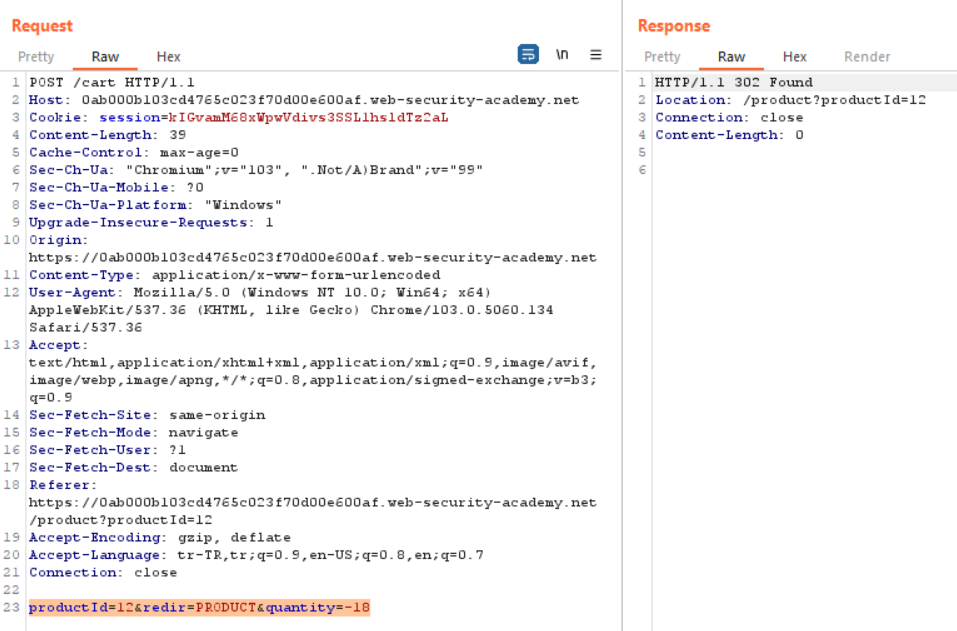
This lab doesn't adequately validate user input. You can exploit a logic flaw in its purchasing workflow to buy items for an unintended price. To solve the lab, buy a "Lightweight l33t leather jacket". You can log in to your own account using the following credentials: wiener:peter [**Access the lab**](https://portswigger.net/academy/labs/launch/8593e55b788d1c4403ccad45020972079a8e89c5669ecf6d9be2cd5c69c77877?referrer=%2fweb-security%2flogic-flaws%2fexamples%2flab-logic-flaws-high-level)

**Solution**

1. With Burp running, log in and add a cheap item to your cart.
2. In Burp, go to "Proxy" > "HTTP history" and study the corresponding HTTP messages. Notice that the quantity is determined by a parameter in the POST /cart request.
3. Go to the "Intercept" tab and turn on interception. Add another item to your cart and go to the intercepted POST /cart request in Burp.
4. Change the quantity parameter to an arbitrary integer, then forward any remaining requests. Observe that the quantity in the cart was successfully updated based on your input.
5. Repeat this process, but request a negative quantity this time. Check that this is successfully deducted from the cart quantity.
6. Request a suitable negative quantity to remove more units from the cart than it currently contains. Confirm that you have successfully forced the cart to contain a negative quantity of the product. Go to your cart and notice that the total price is now also a negative amount.
7. Add the leather jacket to your cart as normal. Add a suitable negative quantity of the another item to reduce the total price to less than your remaining store credit.
8. Place the order to solve the lab.



Mantıksal yanlışlık buradan görülebilir



Lab 3: Inconsistent security controls

**APPRENTICE**

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 Carlos.

[**Access the lab**](https://portswigger.net/academy/labs/launch/07b14e865f15e49f0856ab8db29ab190045abf578eff9ee7a794692eb305a391?referrer=%2fweb-security%2flogic-flaws%2fexamples%2flab-logic-flaws-inconsistent-security-controls)

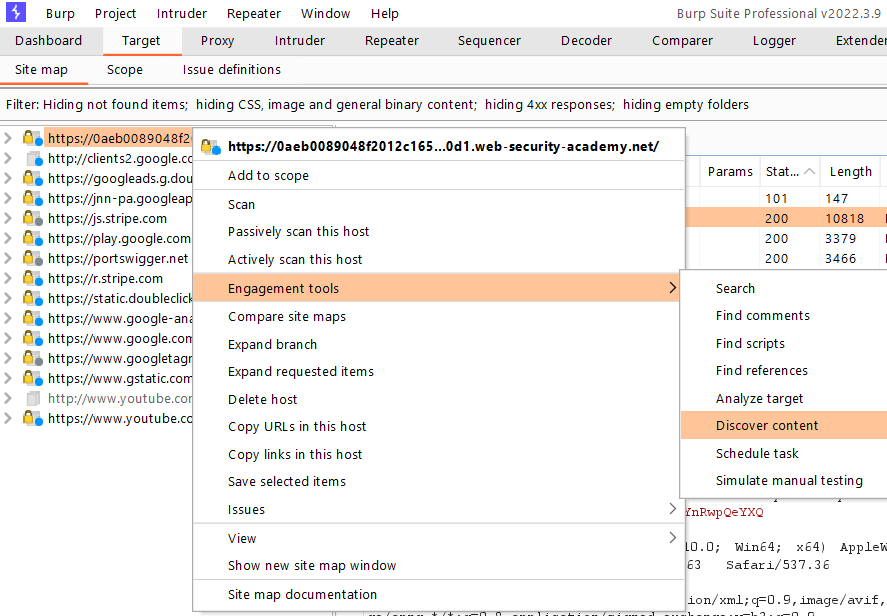
**Solution**

1. Open the lab then go to the "Target" > "Site map" tab in Burp. Right-click on the lab domain and select "Engagement tools" > "Discover content" to open the content discovery tool.
2. Click "Session is not running" to start the content discovery. After a short while, look at the "Site map" tab in the dialog. Notice that it discovered the path /admin.
3. Try and browse to /admin. Although you don't have access, the error message indicates that DontWannaCry users do.
4. Go to the account registration page. Notice the message telling DontWannaCry employees to use their company email address. Register with an arbitrary email address in the format:

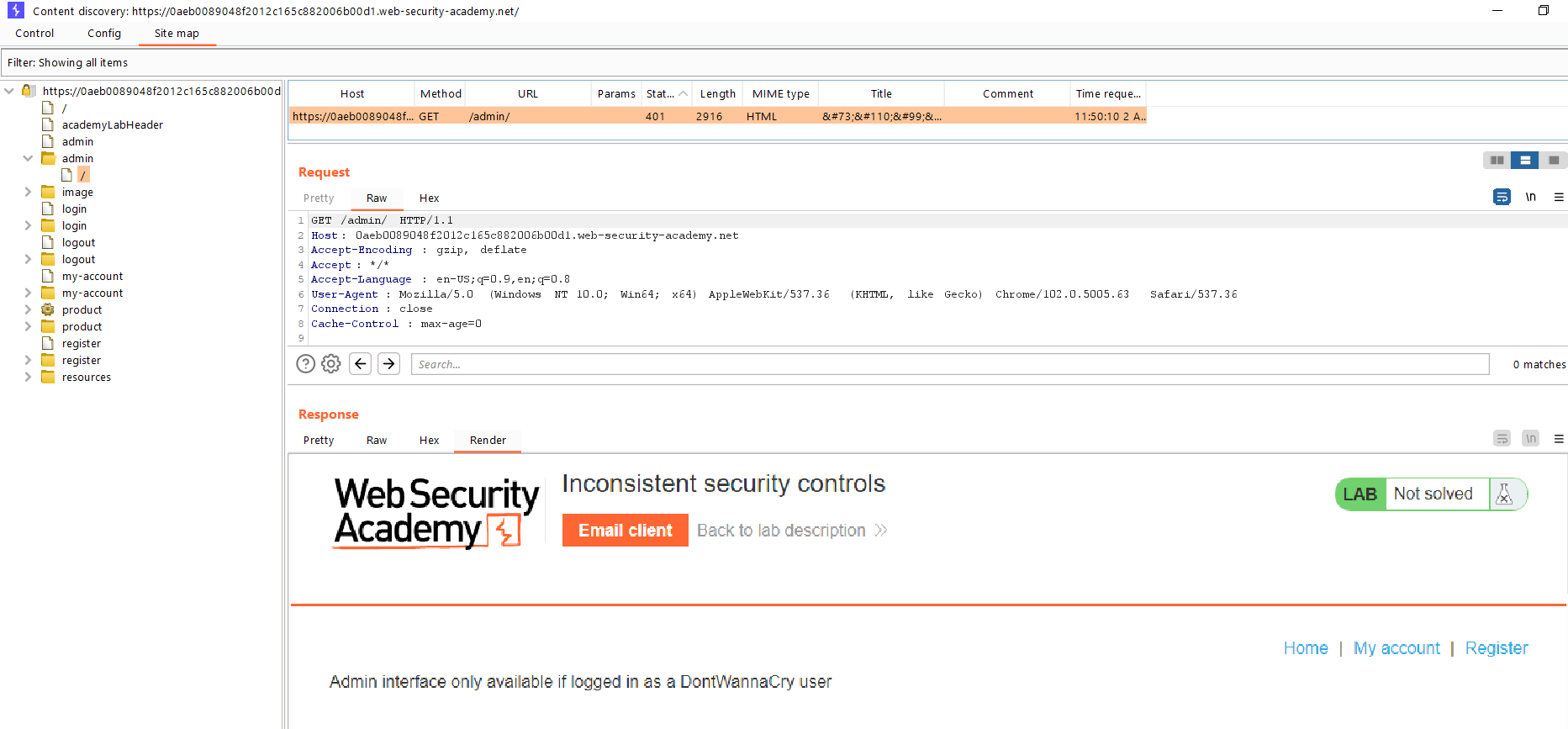
anything@your-email-id.web-security-academy.net

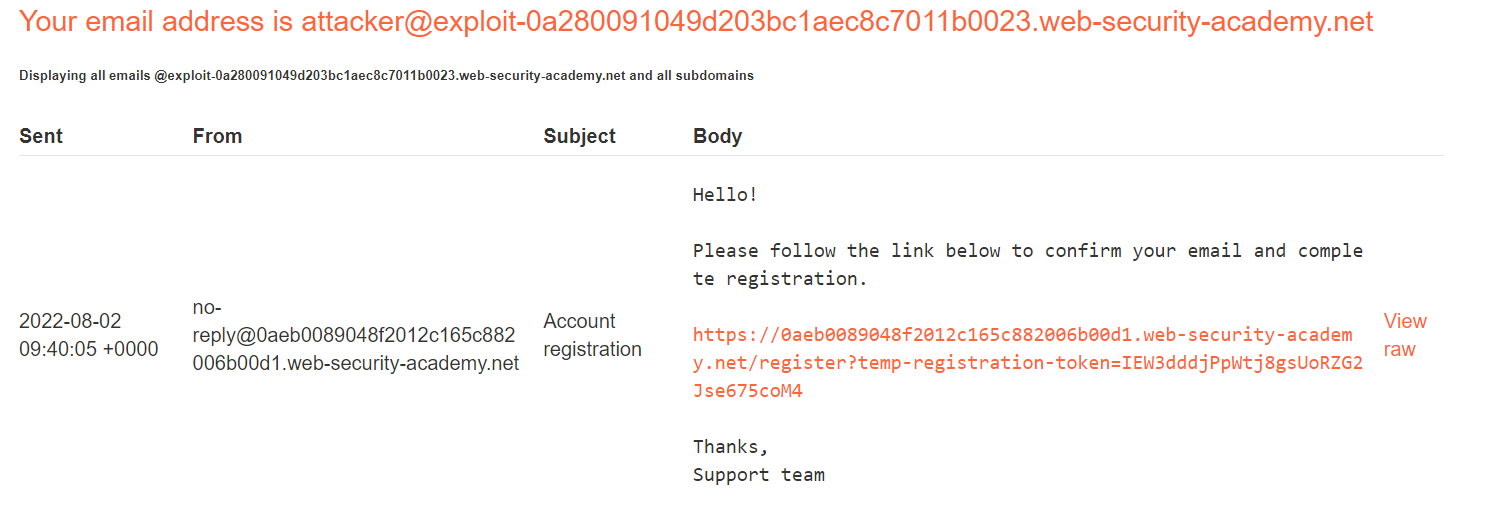
You can find your email domain name by clicking the "Email client" button.

1. Go to the email client and click the link in the confirmation email to complete the registration.
2. Log in using your new account and go to the "My account" page. Notice that you have the option to change your email address. Change your email address to an arbitrary @dontwannacry.com address.
3. Notice that you now have access to the admin panel, where you can delete Carlos to solve the lab.

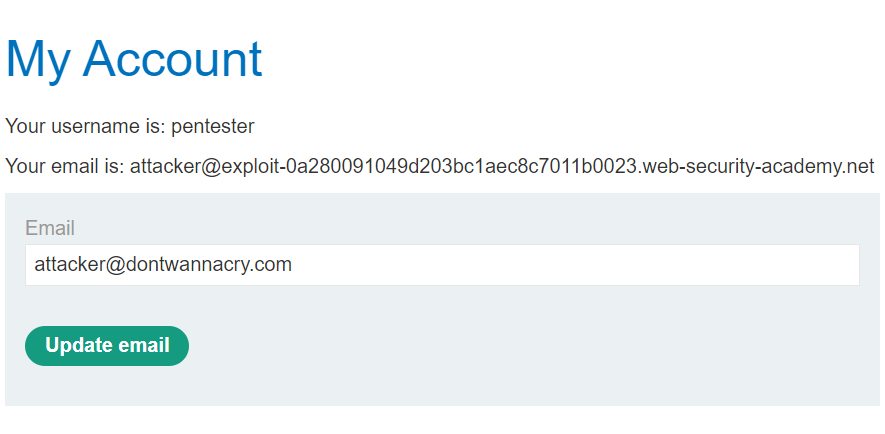


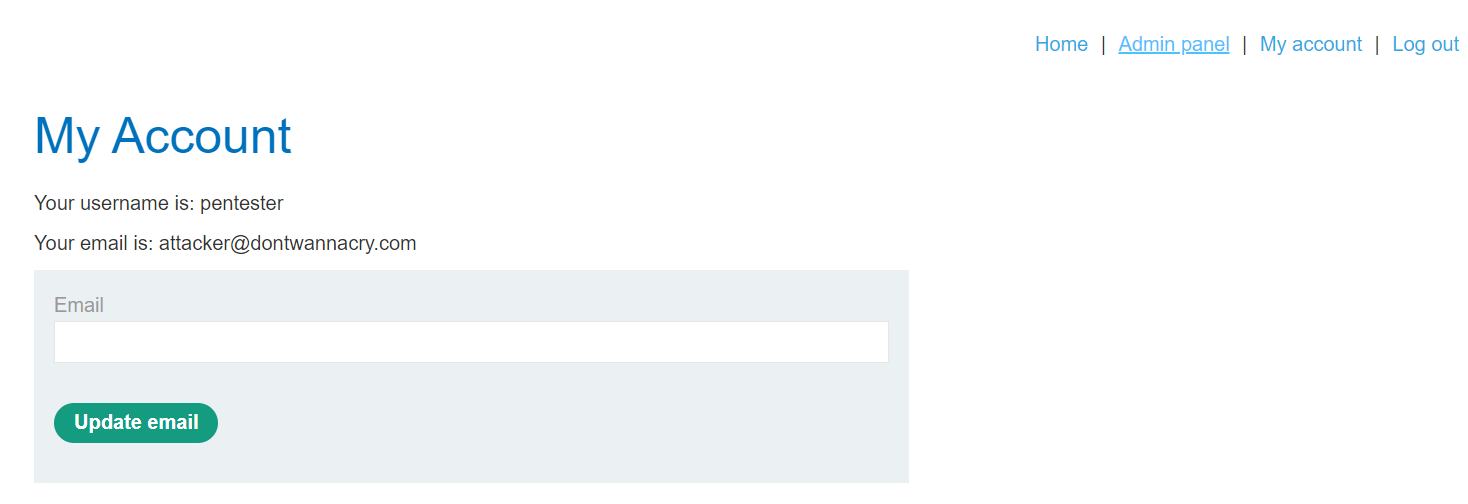
Click the session isnot running button then come back to site map you will see admin request path,we hava DontWannaCry user





Kayıt olurken sana yeni bir email adresi veriyor, o adresi admininkiyle değiştirip admin yetkisine sahip oluyorsun, doğrulama falan yok, saçma yani. Engagement toolsdan sitenin bütün requestlerini çıkarmayı öğrenmiş olduk en azından.





Lab 4: Flawed enforcement of business rules

**APPRENTICE**

This lab has a logic flaw in its purchasing workflow. To solve the lab, exploit this flaw to buy a "Lightweight l33t leather jacket".

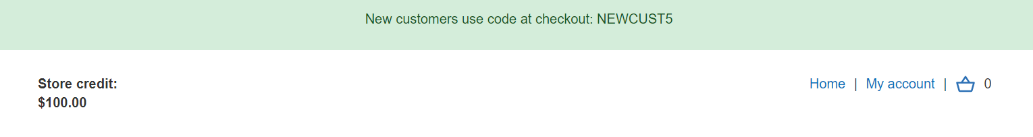
You can log in to your own account using the following credentials: wiener:peter

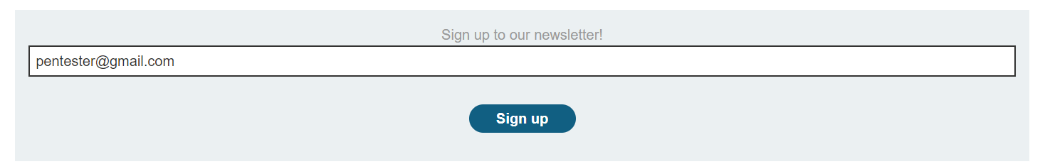
[**Access the lab**](https://portswigger.net/academy/labs/launch/ce7411a23ddad977fdc192a1a252b8737d674481920a71bc5fd307bb5a53aa77?referrer=%2fweb-security%2flogic-flaws%2fexamples%2flab-logic-flaws-flawed-enforcement-of-business-rules)

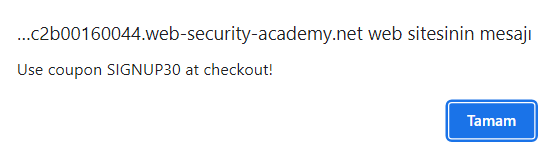
**Solution**

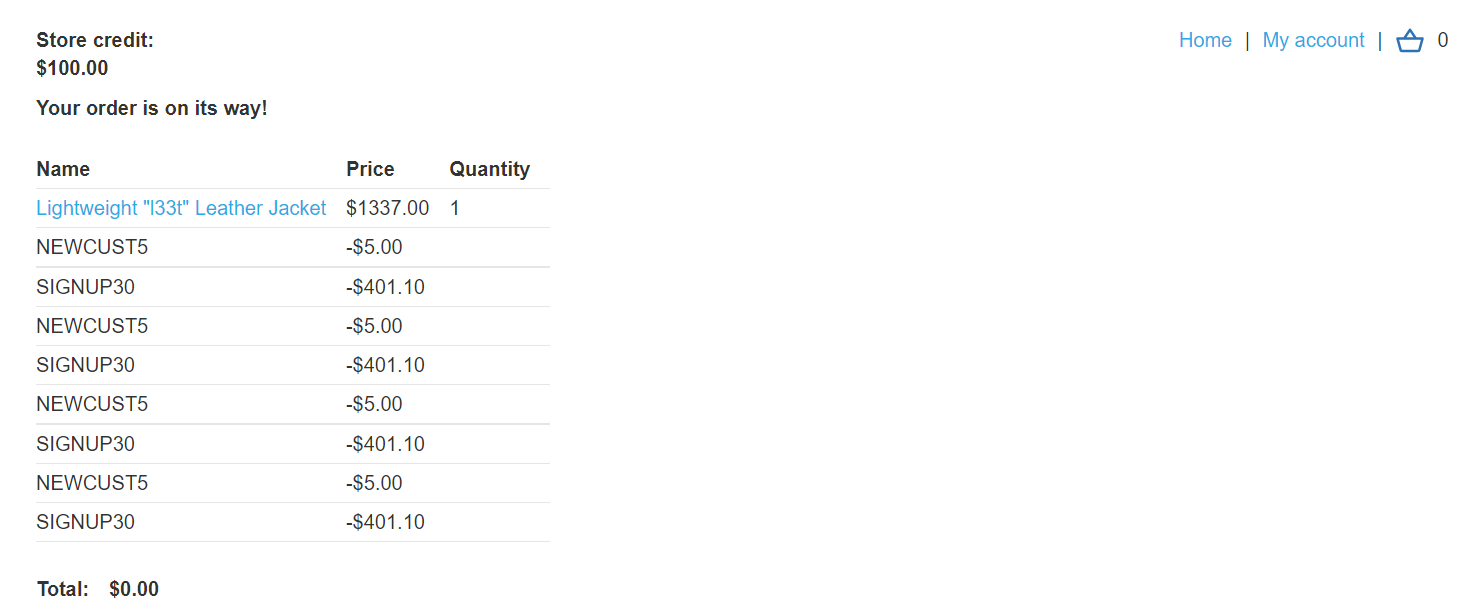
1. Log in and notice that there is a coupon code, NEWCUST5.
2. At the bottom of the page, sign up to the newsletter. You receive another coupon code, SIGNUP30.
3. Add the leather jacket to your cart.
4. Go to the checkout and apply both of the coupon codes to get a discount on your order.
5. Try applying the codes more than once. Notice that if you enter the same code twice in a row, it is rejected because the coupon has already been applied. However, if you alternate between the two codes, you can bypass this control.
6. Reuse the two codes enough times to reduce your order total to less than your remaining store credit. Complete the order to solve the la

Kupon kodlarını değişmeli uyguladığın zaman aynı kupona tekrar indirim uygulatabiliyorsun, açık bu, bir kere uygulanabilmesi lazım









Lab 5: Low-level logic flaw

**PRACTITIONER**

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 l33t leather jacket".

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

**Hint**

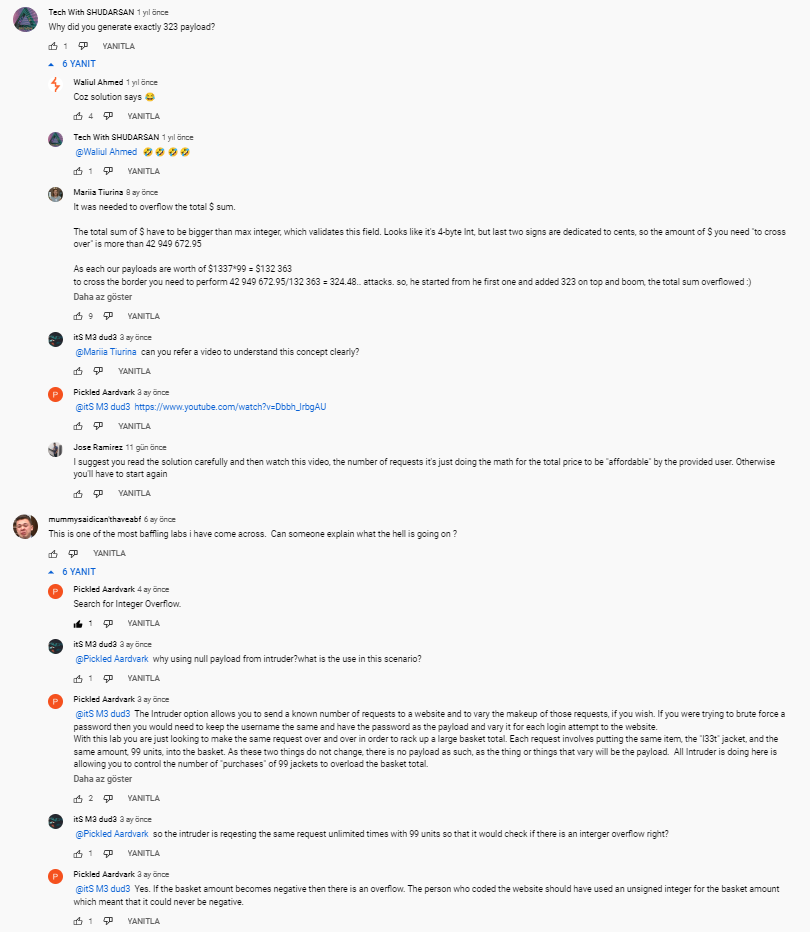
You will need to use Burp Intruder (or Turbo Intruder) to solve this lab.

To make sure the price increases in predictable increments, we recommend configuring your attack to only send one request at a time. In Burp Intruder, you can do this from the resource pool settings using the **Maximum concurrent requests** option.

[**Access the lab**](https://portswigger.net/academy/labs/launch/7d3ebe9916b96a36642a8bd0179888fbcddef63a401c684a077d9877a0966aa4?referrer=%2fweb-security%2flogic-flaws%2fexamples%2flab-logic-flaws-low-level)

**Solution**

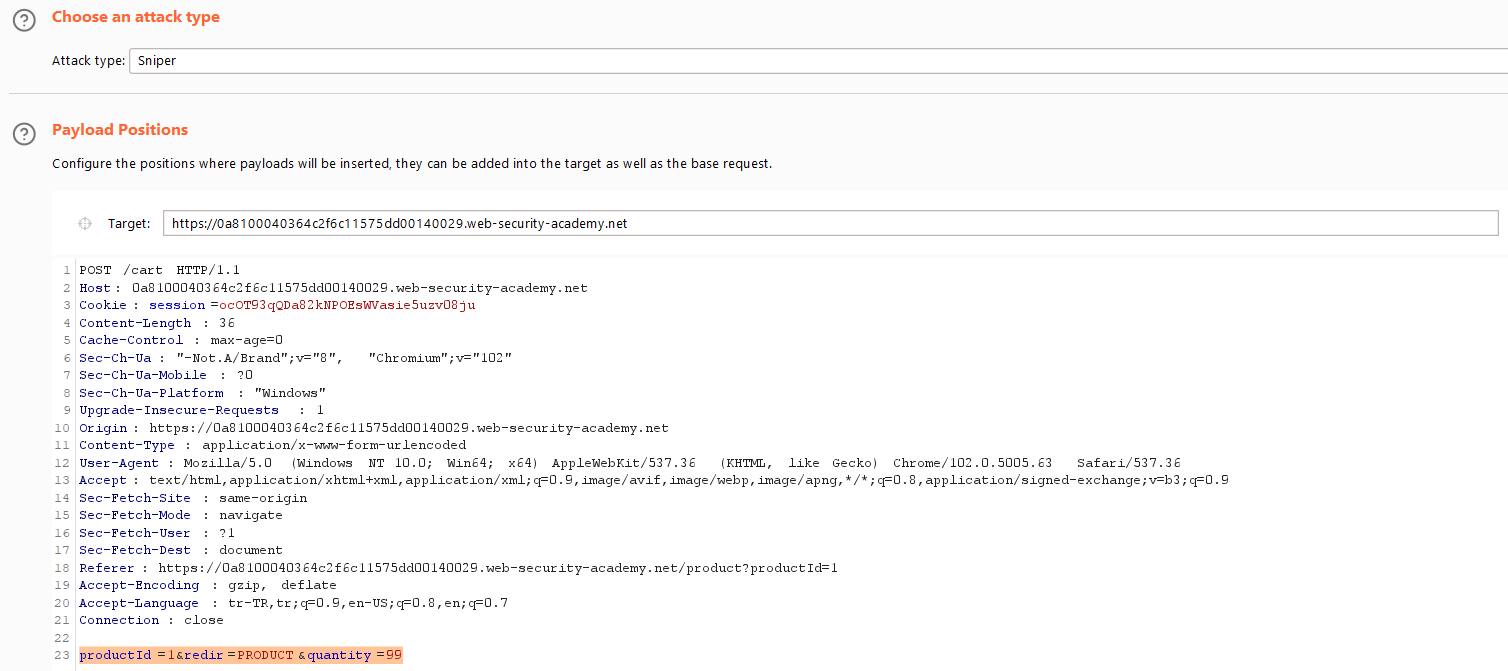
1. With Burp running, log in and attempt to buy the leather jacket. The order is rejected because you don't have enough store credit. In the proxy history, study the order process. Send the POST /cart request to Burp Repeater.
2. In Burp Repeater, notice that you can only add a 2-digit quantity with each request. Send the request to Burp Intruder.
3. Go to Burp Intruder. On the "Positions" tab, clear all the default payload positions and set the quantity parameter to 99.
4. On the "Payloads" tab, select the payload type "Null payloads". Under "Payload options", select "Continue indefinitely". Start the attack.
5. While the attack is running, go to your cart. Keep refreshing the page every so often and monitor the total price. Eventually, notice that the price suddenly switches to a large negative integer and starts counting up towards 0. The price has exceeded the maximum value permitted for an integer in the back-end programming language (2,147,483,647). As a result, the value has looped back around to the minimum possible value (-2,147,483,648).
6. Clear your cart. In the next few steps, we'll try to add enough units so that the price loops back around and settles between $0 and the $100 of your remaining store credit. This is not mathematically possible using only the leather jacket.
7. Create the same Intruder attack again, but this time, under "Payloads" > "Payload Options", choose to generate exactly 323 payloads.
8. Go to the "Resource pool" tab and add the attack to a resource pool with the "Maximum concurrent requests" set to 1. Start the attack.
9. When the Intruder attack finishes, go to the POST /cart request in Burp Repeater and send a single request for 47 jackets. The total price of the order should now be -$1221.96.
10. Use Burp Repeater to add a suitable quantity of another item to your cart so that the total falls between $0 and $100.

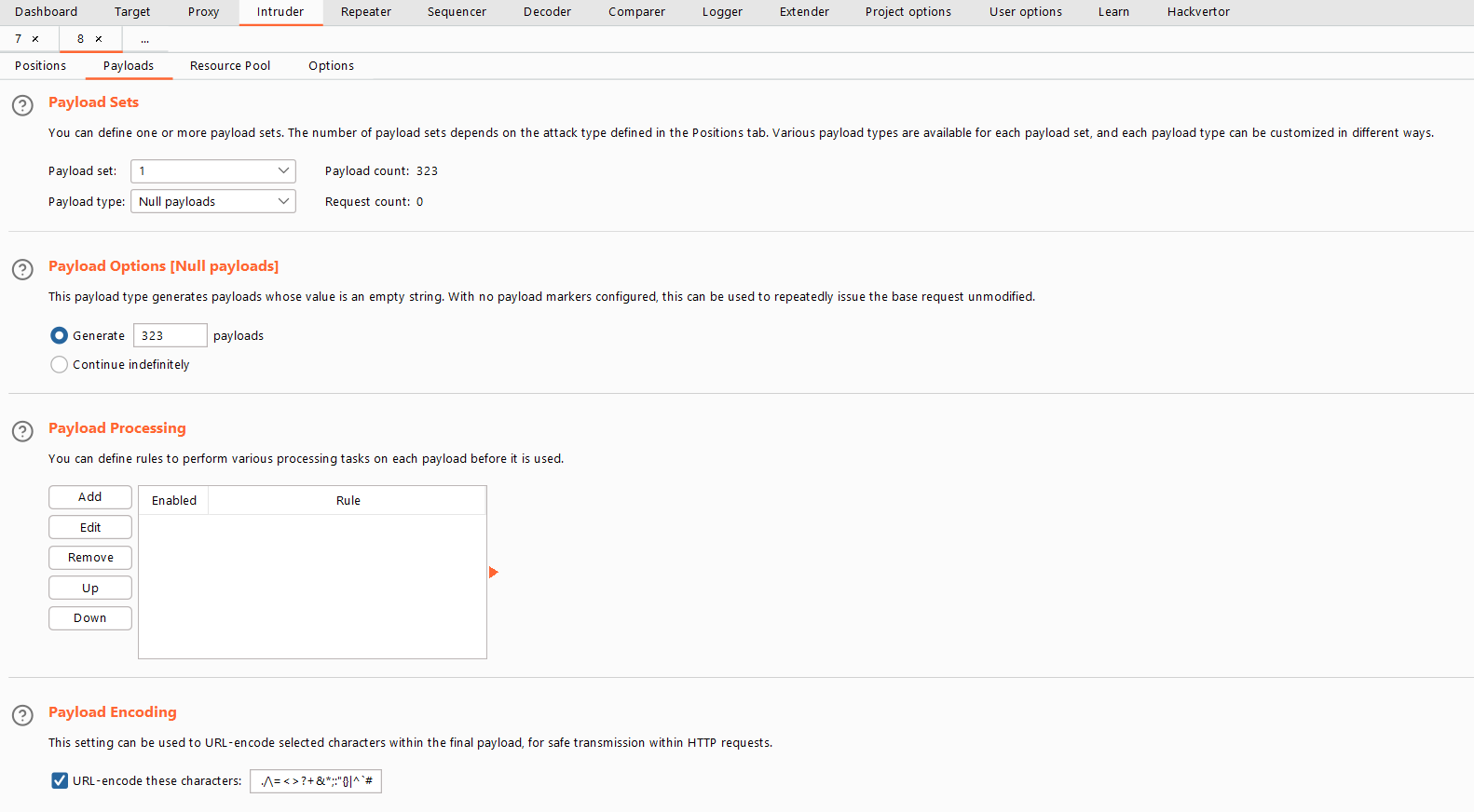


Integer overflow: <https://www.youtube.com/watch?v=Dbbh_lrbgAU&ab_channel=MarcusHutchins>

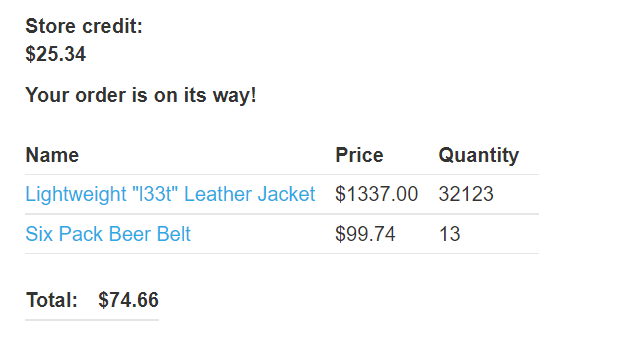
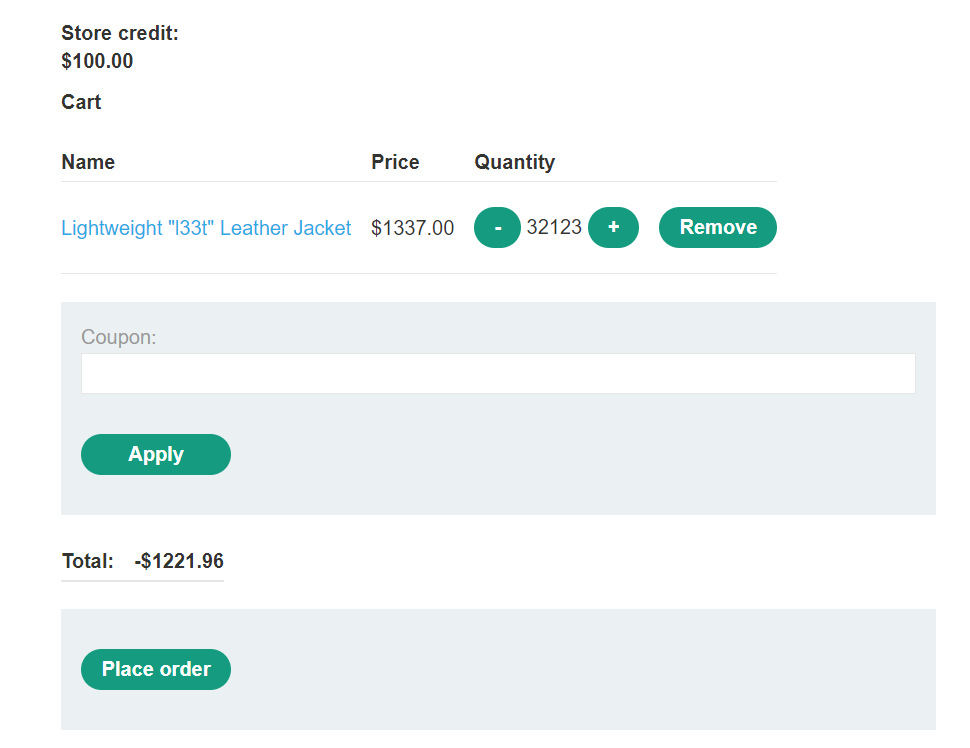
Ceketten miktar olarak 99 yapıyorsun ve sepete ekliyorsun 100 e izin vermiyor.

Sonra bu requesti intrudera atıyorsun. 323 adet null payload yapıyorsun. Her seferinde 1 request olacak şekilde. Sniper attack





Miktar bi süre sonra sayfayı yenileyince eksiye düşüyor.



Başka ürün ekleyerek total price ı artıya geçiriyorsun.

Lab 7: Weak isolation on dual-use endpoint

**PRACTITIONER**

This lab makes a flawed assumption about the user's privilege level based on their input. As a result, you can exploit the logic of its account management features to gain access to arbitrary users' accounts. To solve the lab, access the administrator account and delete Carlos.

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

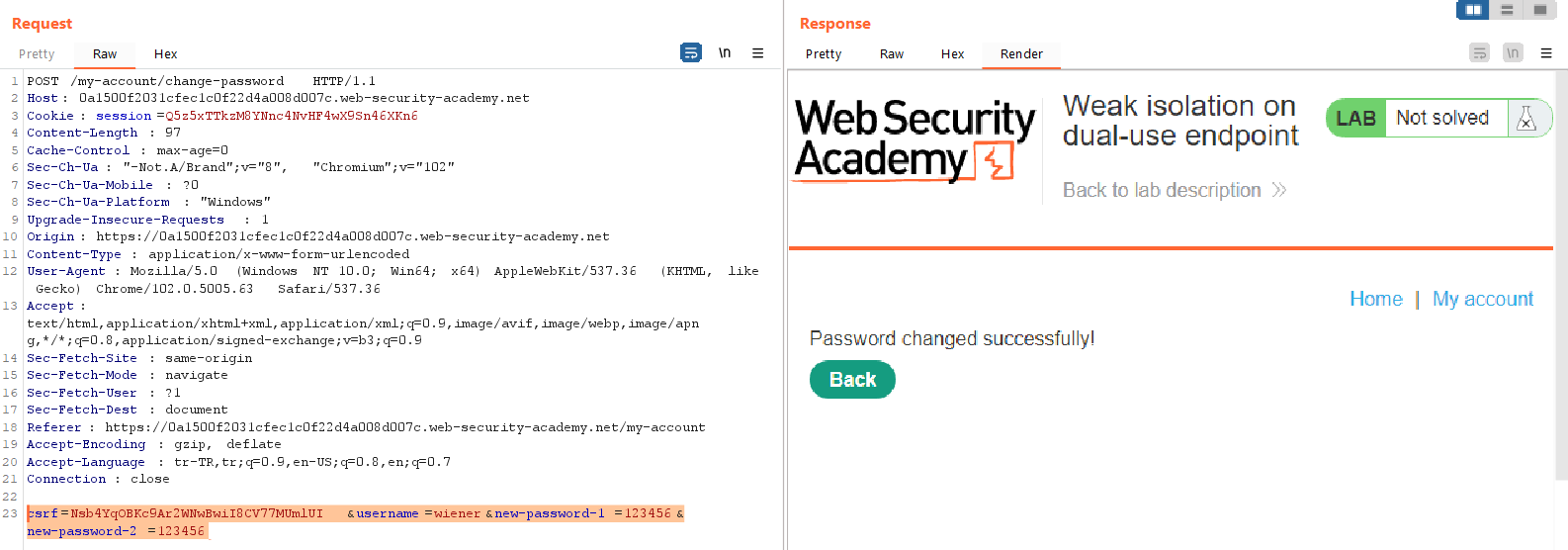
[**Access the lab**](https://portswigger.net/academy/labs/launch/05a619f04b486230a3144985ade21e739b2d88052bb72e902cd033c906b991e3?referrer=%2fweb-security%2flogic-flaws%2fexamples%2flab-logic-flaws-weak-isolation-on-dual-use-endpoint)

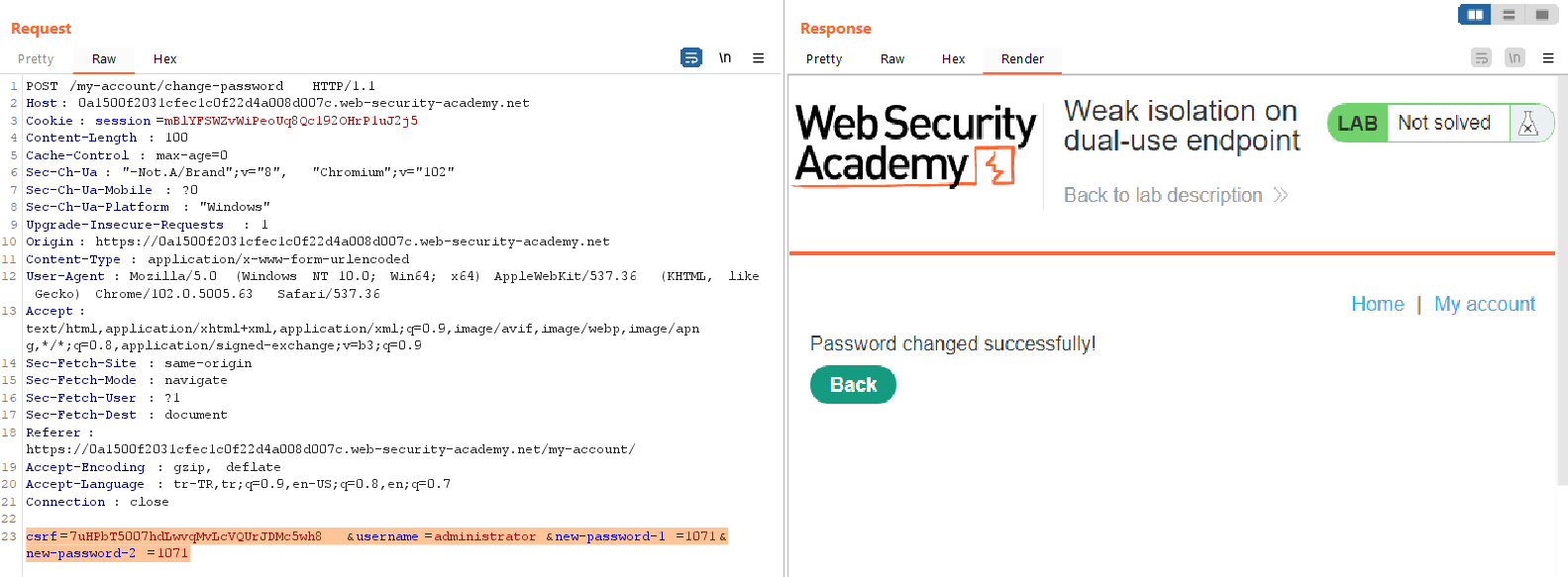
**Solution**

1. With Burp running, log in and access your account page.
2. Change your password.
3. Study the POST /my-account/change-password request in Burp Repeater.
4. Notice that if you remove the current-password parameter entirely, you are able to successfully change your password without providing your current one.
5. Observe that the user whose password is changed is determined by the username parameter. Set username=administrator and send the request again.
6. Log out and notice that you can now successfully log in as the administrator using the password you just set.
7. Go to the admin panel and delete Carlos to solve the lab.

Şifreyi değiştirirken current password alanını silip requesti gönderirsen şifreyi değiştirebiliyorsun,

Yani administratorun şifresini bilmeden şifre değiştirebiliyorsun.





Lab 8: Insufficient workflow validation

**PRACTITIONER**

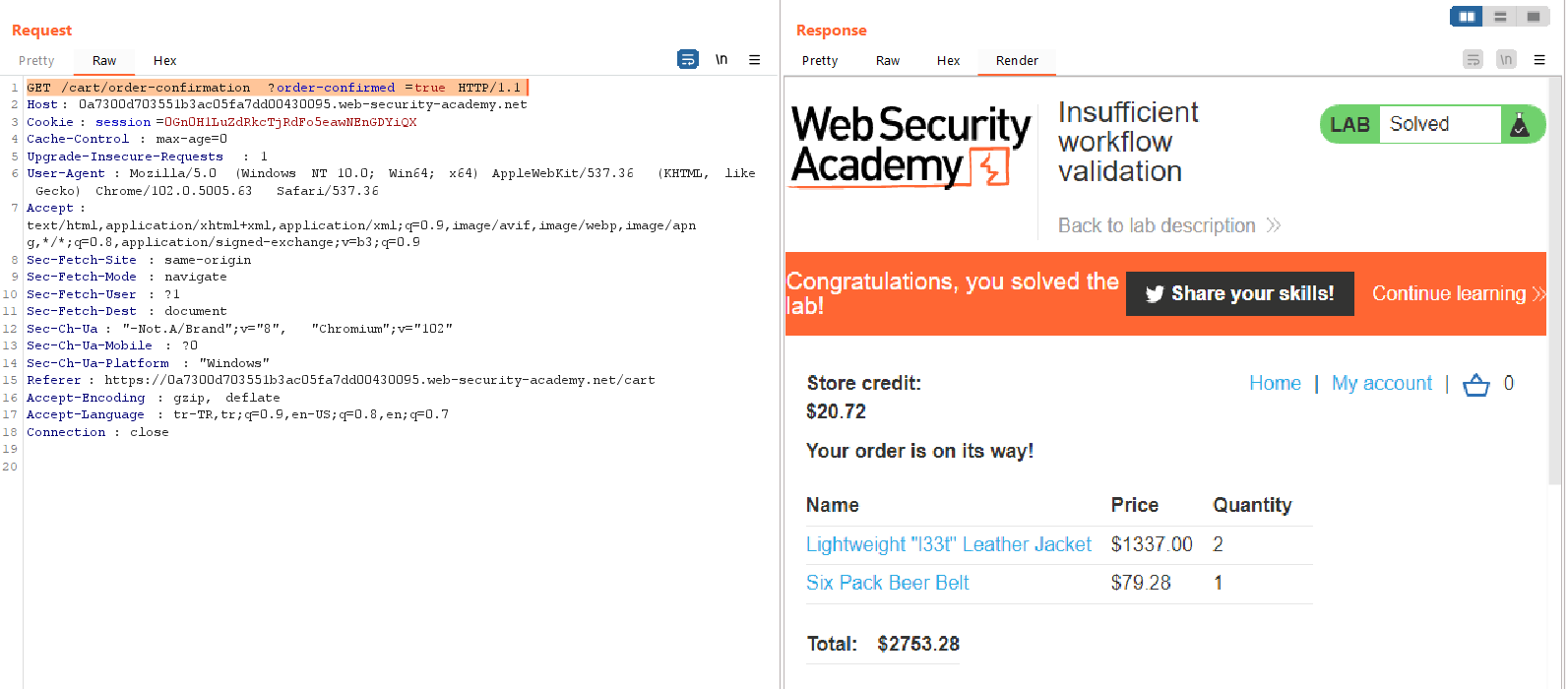
This lab makes flawed assumptions about the sequence of events in the purchasing workflow. To solve the lab, exploit this flaw to buy a "Lightweight l33t leather jacket". You can log in to your own account using the following credentials: wiener:peter

[**Access the lab**](https://portswigger.net/academy/labs/launch/b20989c23ae664ef4d1f4d060455e20d6c019ae17819049dfad91790a7c55765?referrer=%2fweb-security%2flogic-flaws%2fexamples%2flab-logic-flaws-insufficient-workflow-validation)

**Solution**

1. With Burp running, log in and buy any item that you can afford with your store credit.
2. Study the proxy history. Observe that when you place an order, the POST /cart/checkout request redirects you to an order confirmation page. Send GET /cart/order-confirmation?order-confirmation=true to Burp Repeater.
3. Add the leather jacket to your basket.
4. In Burp Repeater, resend the order confirmation request. Observe that the order is completed without the cost being deducted from your store credit and the lab is solved.

Place order requestini gönderdikten sonra GET /cart/order-confirmation?order-confirmation=true  requesti oluşuyor bunu tutup repeatera gönderip üstüne başka bir ürün ekleyip o tuttuğun requesti gönderdiğin zaman siparişi tamamlayabiliyorsun. Bu durumda confirmotionın süresi önemli oluyor.



100 dolardan az ürün ekle

İntercept place order and forward >oluşan yeni request 🡪 GET /cart/order-confirmation?order-confirmation=true  🡪 send to repeater 🡪

Yeni ürün ekle 🡪 send now GET /cart/order-confirmation?order-confirmation=true

Lab 9: Authentication bypass via flawed state machine

**PRACTITIONER**

This lab makes flawed assumptions about the sequence of events in the login process. To solve the lab, exploit this flaw to bypass the lab's authentication, access the admin interface, and delete Carlos.

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

[**Access the lab**](https://portswigger.net/academy/labs/launch/f009e13156910cf7897bc7ed85b32662e8b2753196347950c3b3c51d86b9c3c5?referrer=%2fweb-security%2flogic-flaws%2fexamples%2flab-logic-flaws-authentication-bypass-via-flawed-state-machine)

**Solution**

1. With Burp running, complete the login process and notice that you need to select your role before you are taken to the home page.
2. Use the content discovery tool to identify the /admin path.
3. Try browsing to /admin directly from the role selection page and observe that this doesn't work.
4. Log out and then go back to the login page. In Burp, turn on proxy intercept then log in.
5. Forward the POST /login request. The next request is GET /role-selector. Drop this request and then browse to the lab's home page. Observe that your role has defaulted to the administrator role and you have access to the admin panel.
6. Delete Carlos to solve the lab

Wiener ve peter ile giriş yapıp bunu intercept ile durdurup forwardladığın zaman role selector geliyor onu düşürüp

<https://0ad000bd0428f328c1ba227b006f00c5.web-security-academy.net/> url sine gittiğimiz zaman admin paneline ulaşmış oluyoruz.

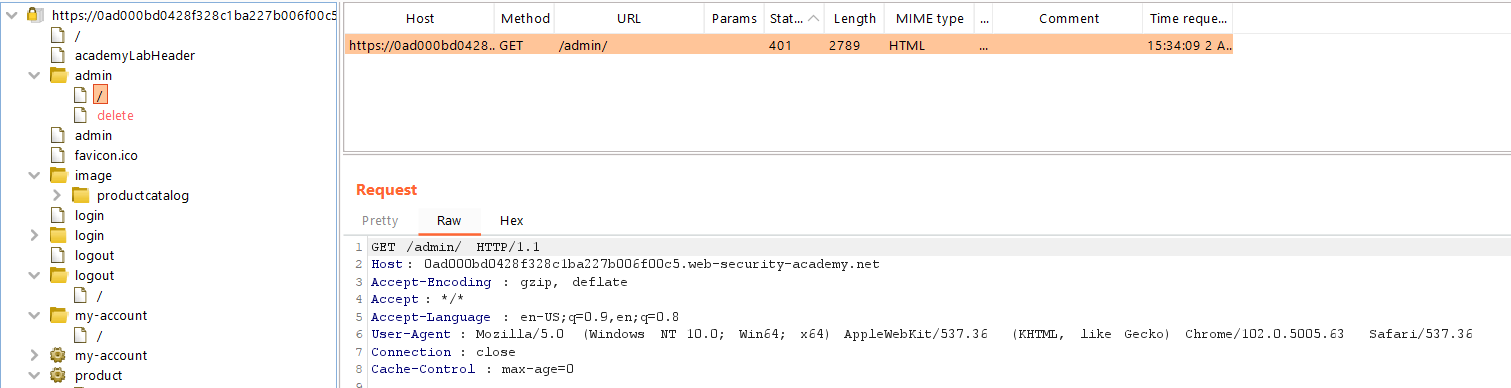


Forward and drop coming request

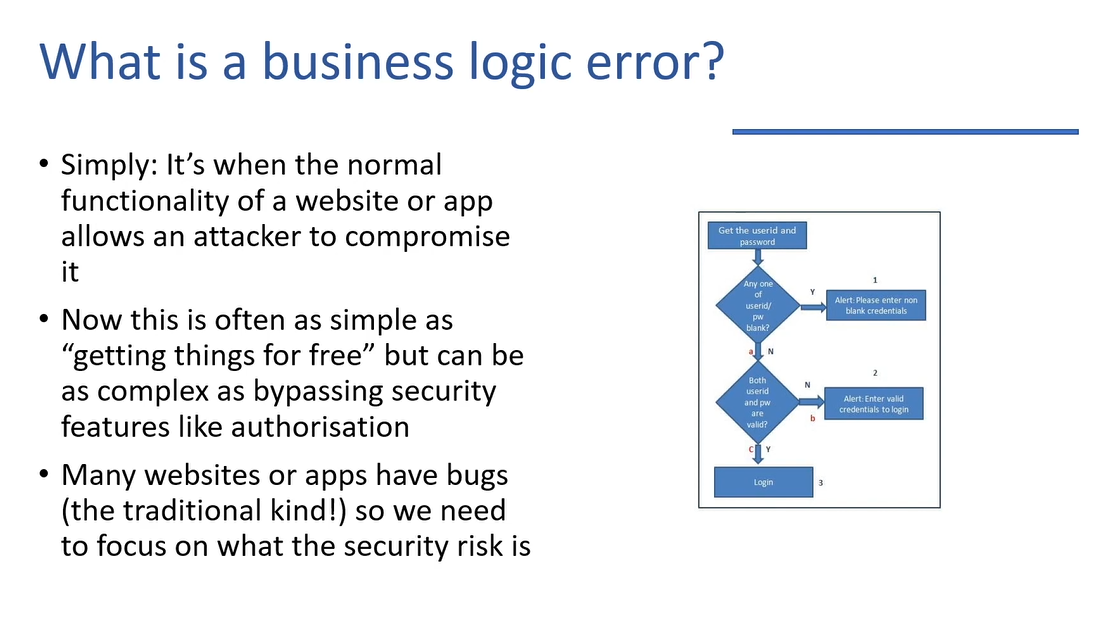
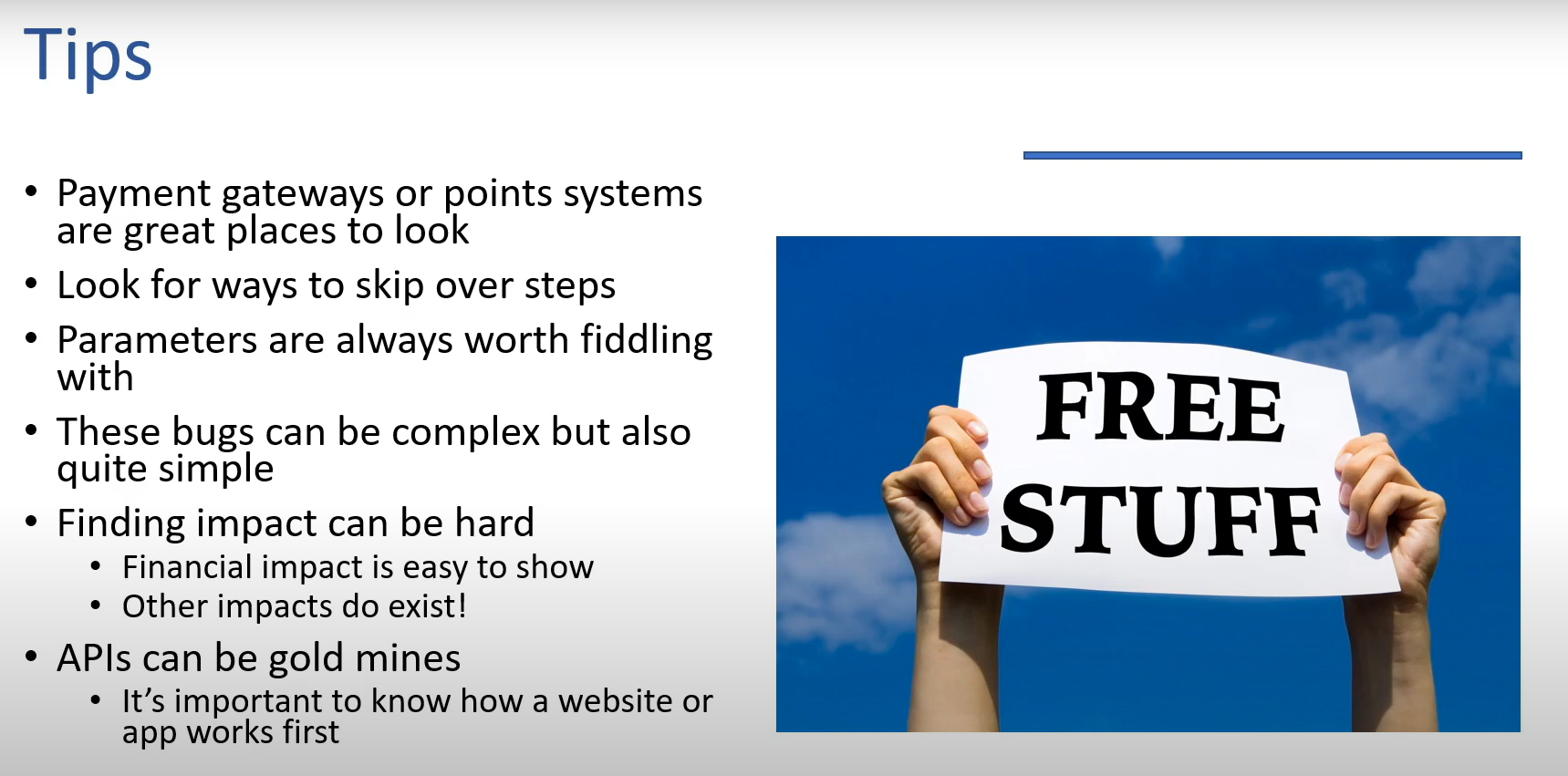
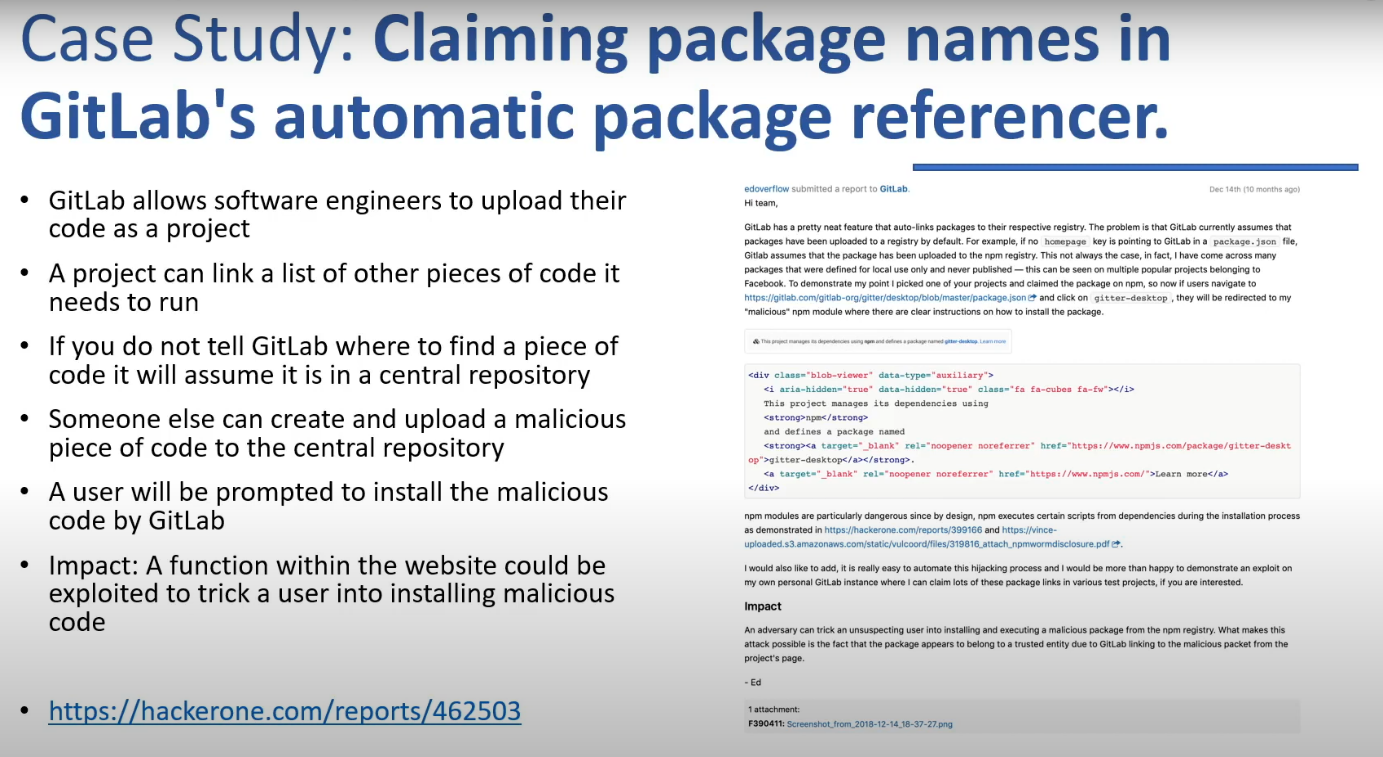
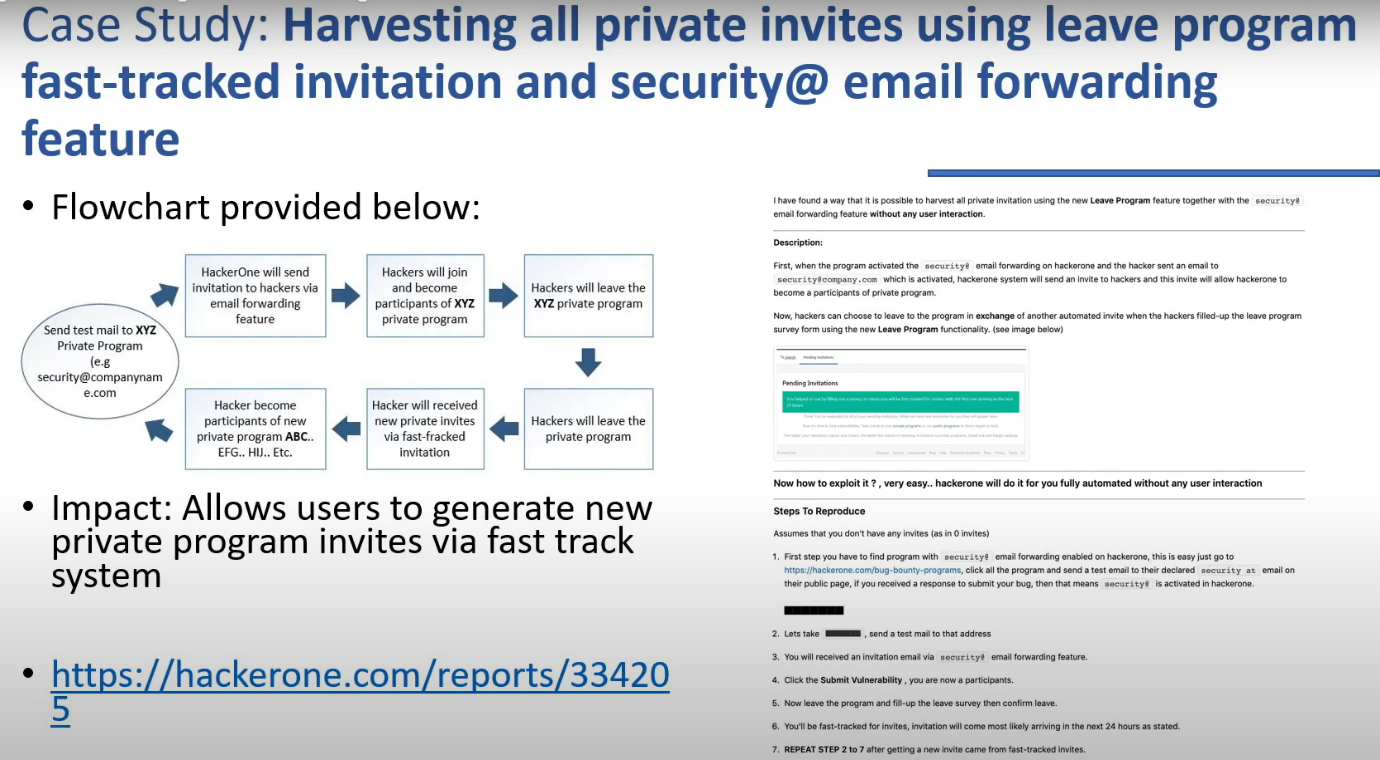
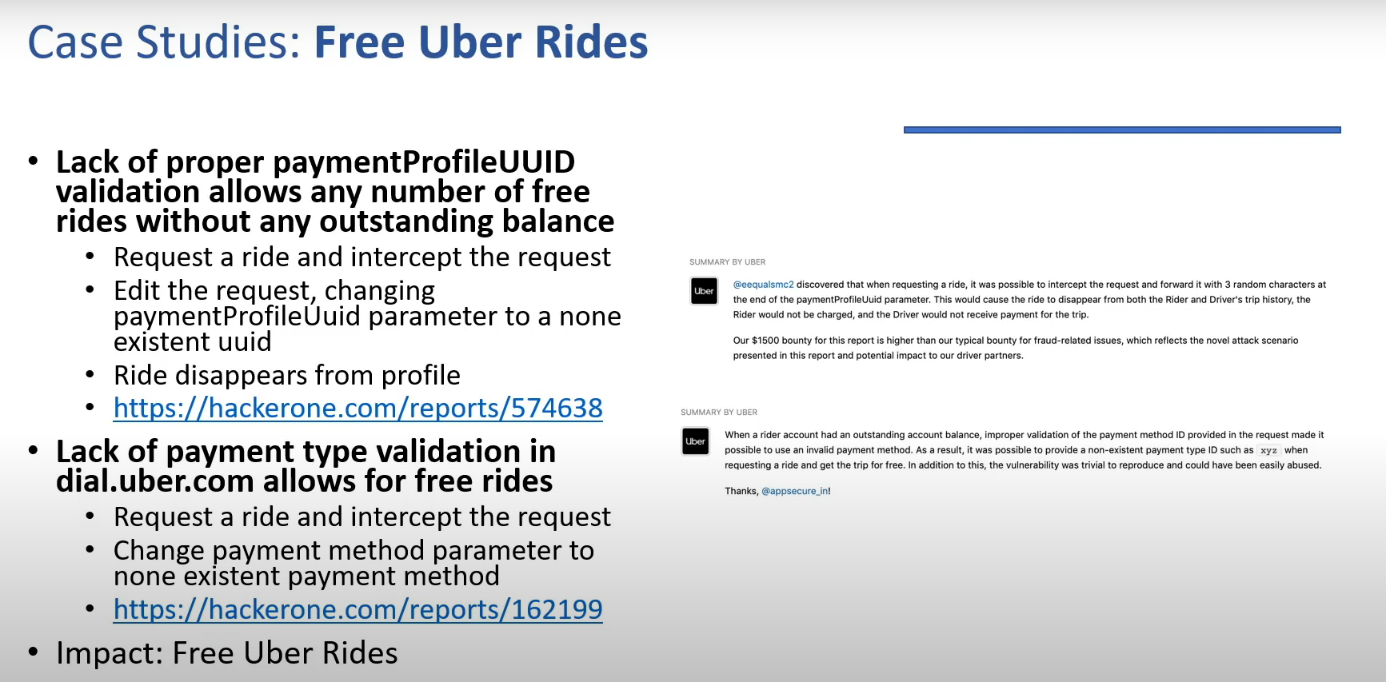
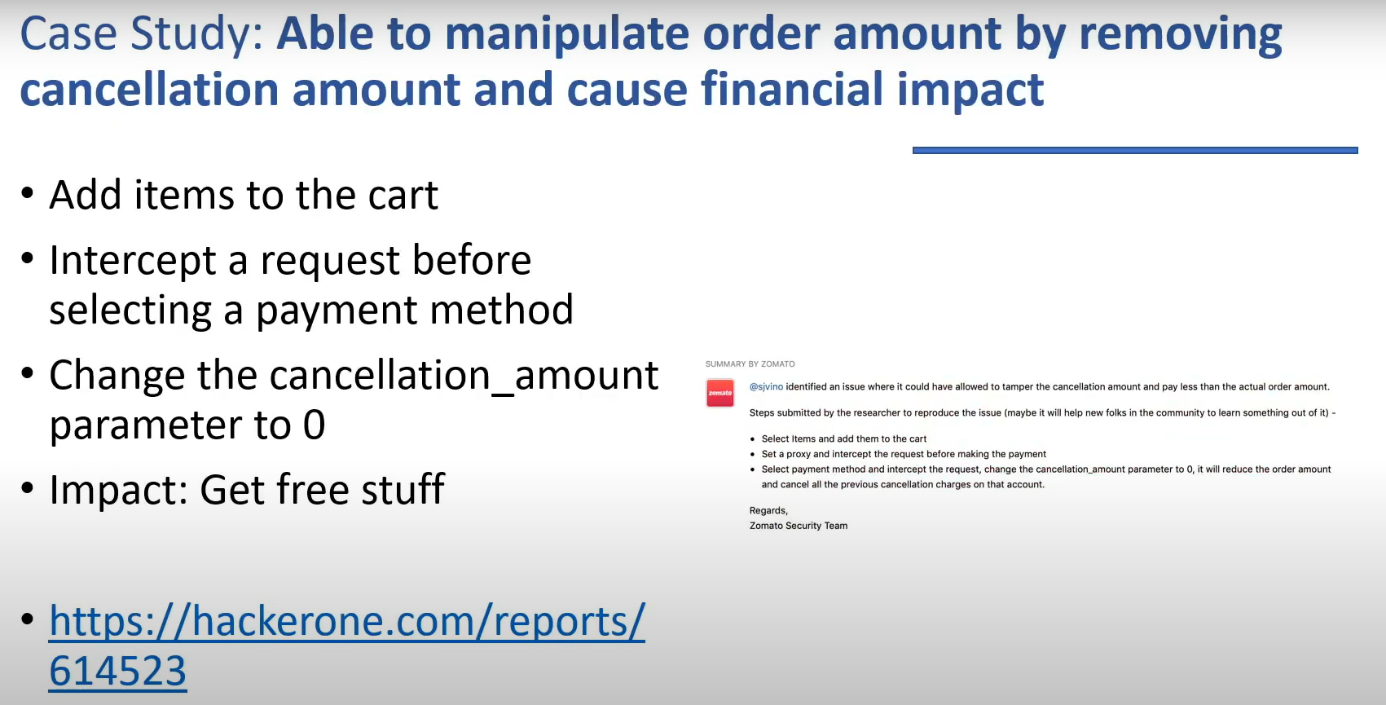
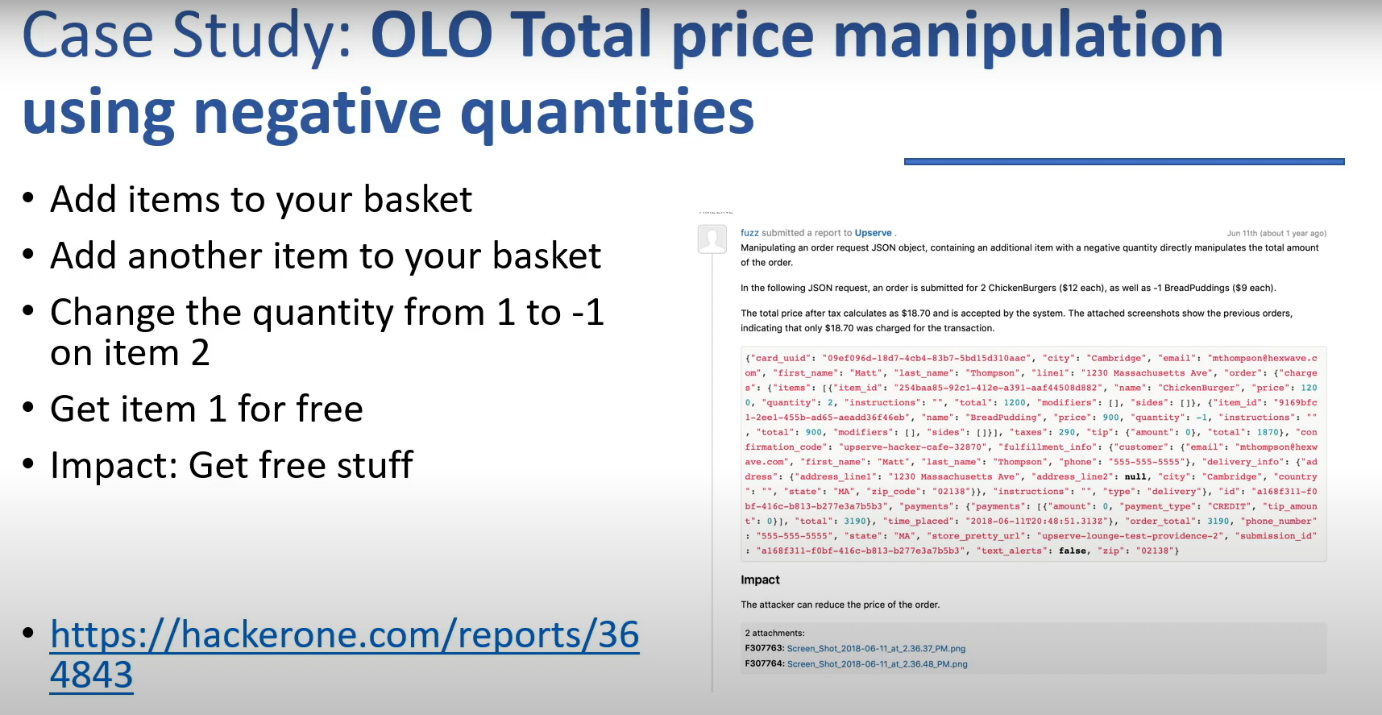
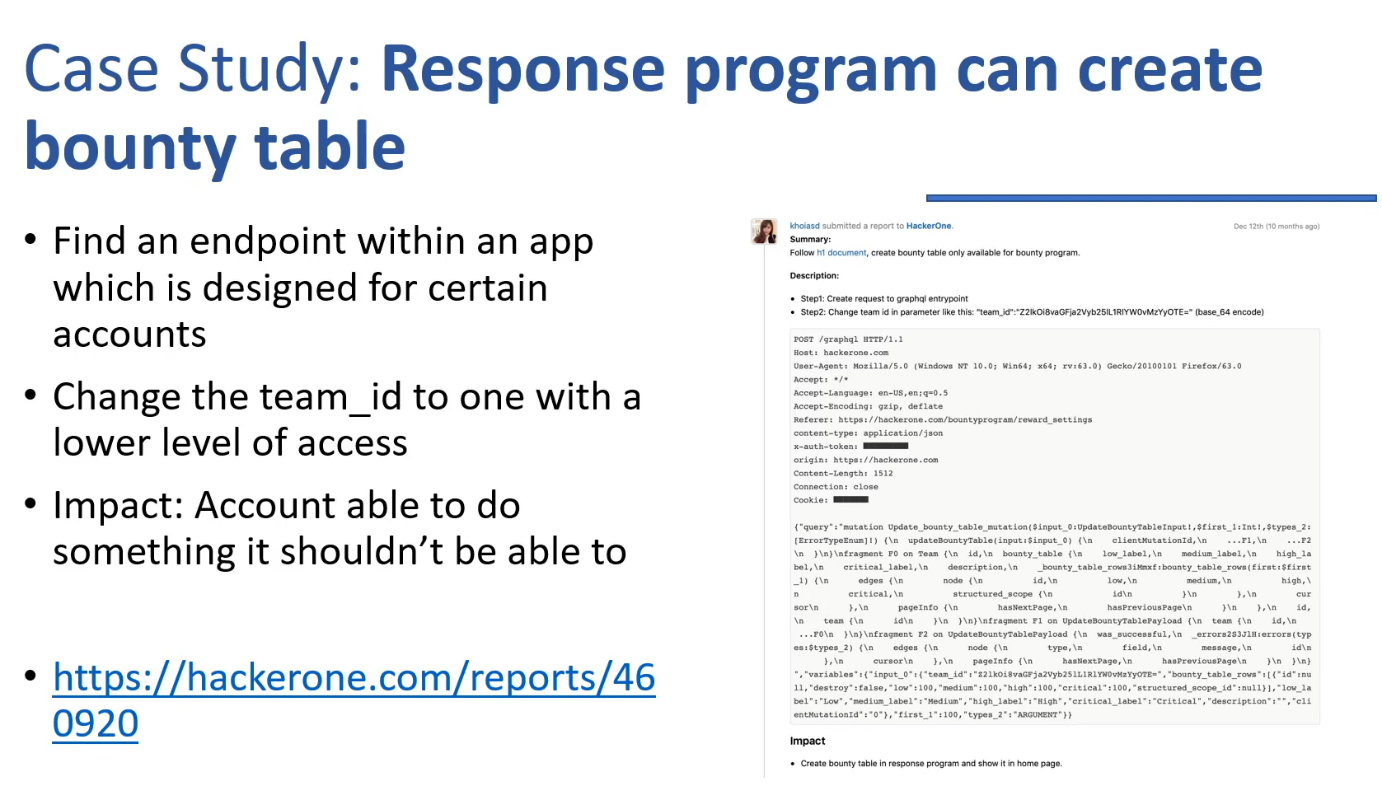
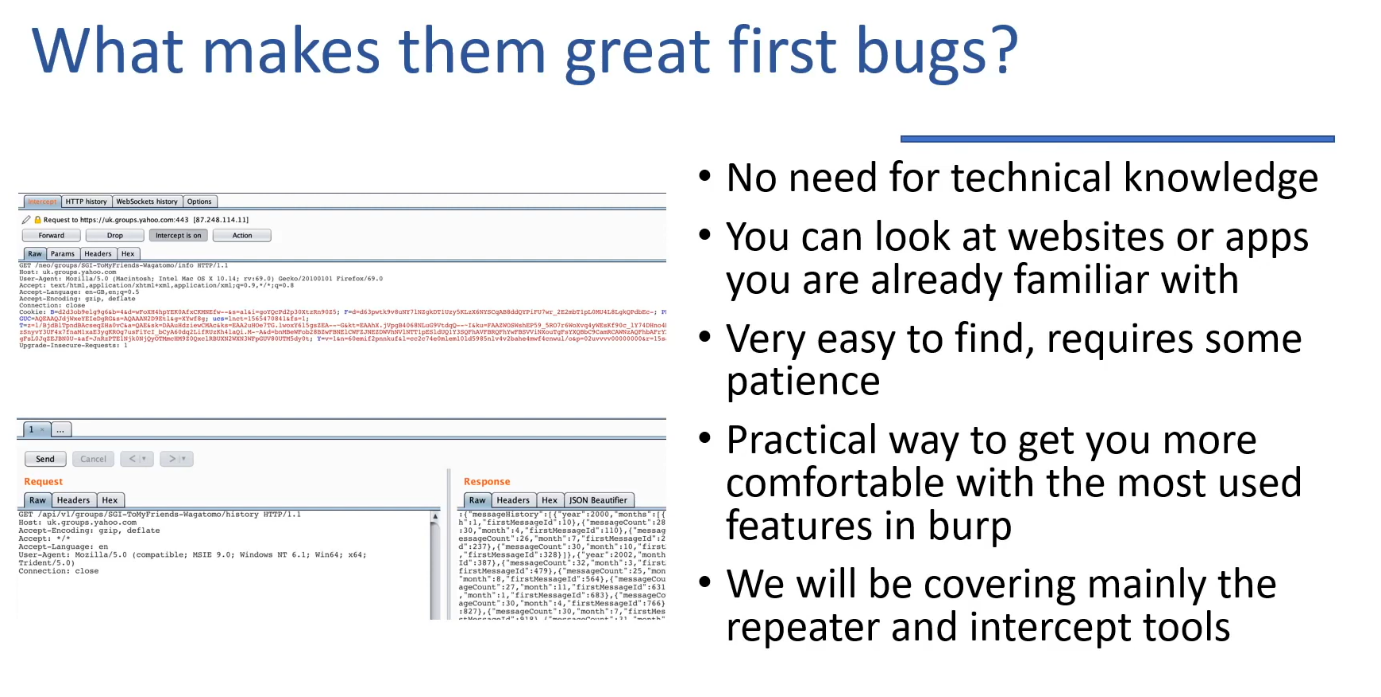


Then go <https://0ad000bd0428f328c1ba227b006f00c5.web-security-academy.net/> you will see the admin panel, you wil be redirect to <https://0ad000bd0428f328c1ba227b006f00c5.web-security-academy.net/admin> and delete carlos.

Aynı zamanda engagement tools dan siteyi tarttığında admin endpointini göreceksin



INFORMATION ABOUT BUSINESS LOGIC VULNERABILITIES

Images from InsiderPhd