

Slovenská technická univerzita v Bratislave  
Fakulta informatiky a informačných technológií

Ilkovičova 2, 842 16 Bratislava 4



# Používateľská príručka pre security e-shop

---

*Tímový projekt*

Tím č. 19

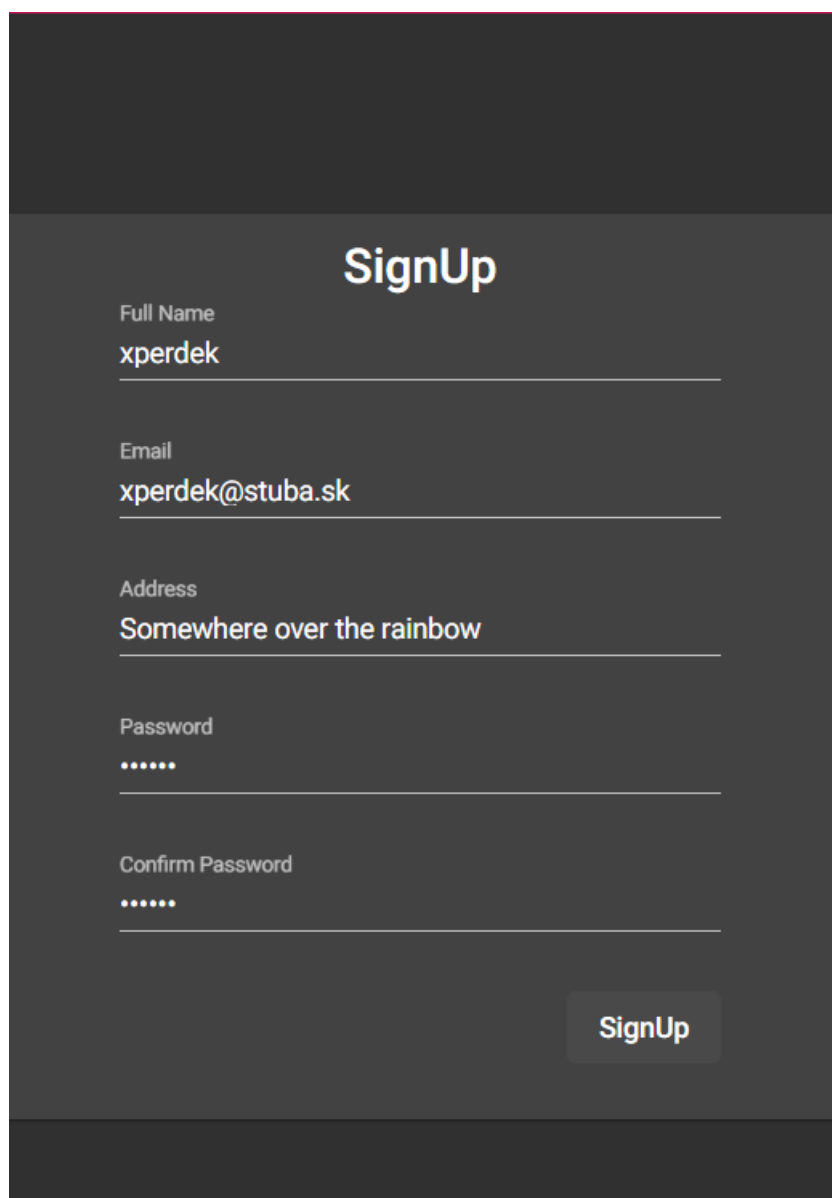
**Vypracoval:** Jakub Perdek

**Vedúci projektu:** Ing. Pavol Helebrandt Phd.

# Registrácia a prihlásenie používateľa

Na začiatku sa používateľ zaregistruje. Vyplní všetky položky registračného formulára. Zapamätá si meno a heslo a uvedie funkčný a jedinečný email. Následne použije meno a heslo pri prihlasovaní. Automaticky mu bude priradená roľa používateľa.

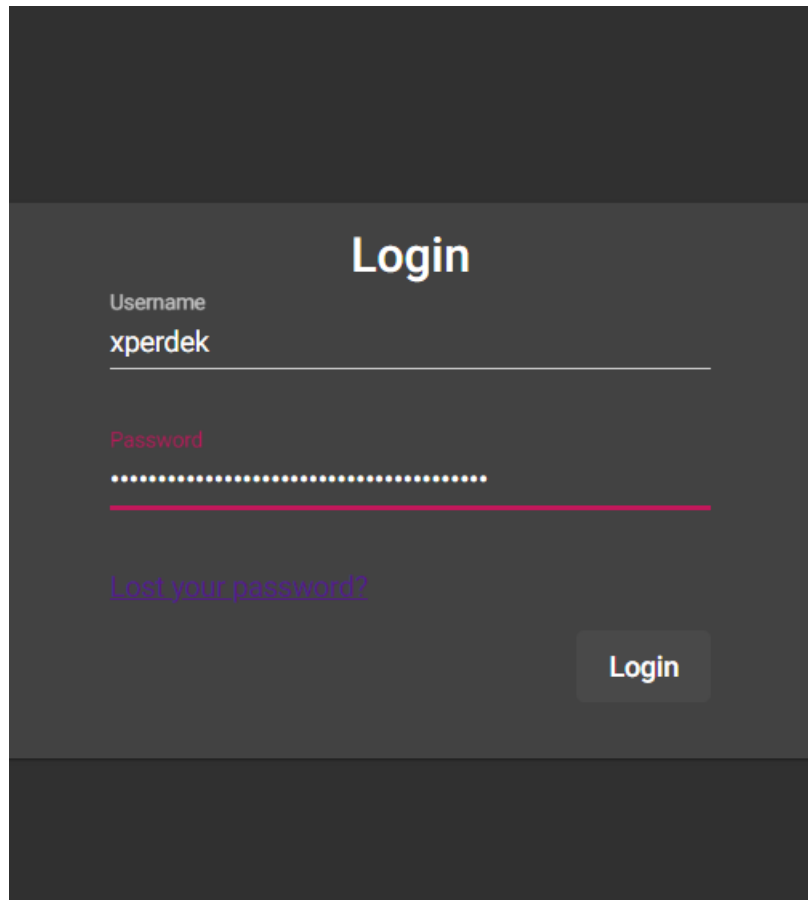
1. Zaregistrujte sa stlačením na tlačidlo SignUp v hornom rohu stránky.



The image shows a dark-themed user registration form. At the top, the title "SignUp" is displayed in a large, white, sans-serif font. Below the title, there are five input fields, each with a label above it: "Full Name", "Email", "Address", "Password", and "Confirm Password". The "Full Name" field contains the text "xperdek". The "Email" field contains "xperdek@stuba.sk". The "Address" field contains "Somewhere over the rainbow". The "Password" and "Confirm Password" fields are filled with six dots each, indicating masked text. At the bottom right of the form, there is a rectangular button with the text "SignUp" in white. The entire form is set against a dark gray background.

Obrázok 1: Registrácia používateľa

2. Následne sa prihláste zadaním vášho používateľského mena a hesla.

A login form with a dark gray background. At the top, the word "Login" is displayed in a large, white, sans-serif font. Below it, there are two input fields. The first is labeled "Username" in a small, light gray font, and the text "xperdek" is entered in white. The second is labeled "Password" in a small, light gray font, and the password is masked with white dots. Below the password field, there is a link that says "Lost your password?" in a light blue font. At the bottom right of the form, there is a white button with the text "Login" in a dark gray font.

Username  
xperdek

Password  
.....

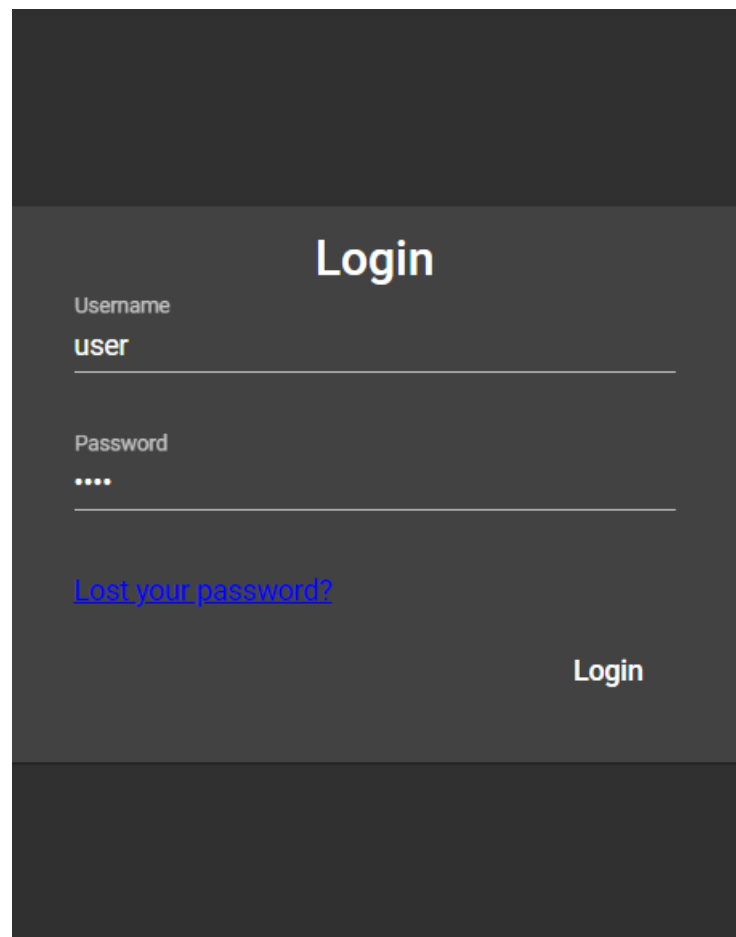
[Lost your password?](#)

Login

Obrázok 2: Prihlásenie používateľa

# Prelamovanie hesiel

Jeden z pracovníkov obchodu má nastavené uhádnuteľné slabé heslo. Princípom tohto scenára je zistiť toto heslo skúšaním rôznych hesiel pre používateľov pomocou ľubovoľného nástroja. Musí to ale realizovať prostredníctvom rozhrania pre Angular. Stačí ak vyskúša jednoduché heslá ručne. Rovnako si môže zistiť hash hesla vytvorený bcryptom vrátený do Angularu pre overenie. Ten môže získať sledovaním premávky. Následne by mohol skúšať známe heslá a porovnávať vytvorené hashe s hashmi vytvorenými pre reťazce na zozname. Túto časť môže realizovať aj offline. Meno a heslo sú rovnaké, a to user a user. Malo by ich preto byť jednoduché zistiť. Často sú na zozname najpoužívanějších hesiel.



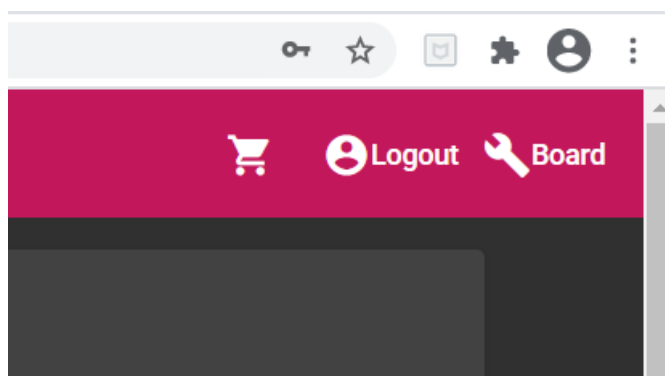
The image shows a dark-themed login interface. At the top, the word "Login" is displayed in a large, white, sans-serif font. Below it, there are two input fields. The first field is labeled "Username" in a small, light gray font, and it contains the text "user" in a white font. The second field is labeled "Password" in a small, light gray font, and it contains four white dots. Below the password field, there is a link that says "Lost your password?" in a blue, underlined font. At the bottom right of the form, there is a white "Login" button.

Obrázok 3: Aplikovanie jednoduchého hesla user

# Použitie SQL injekcie

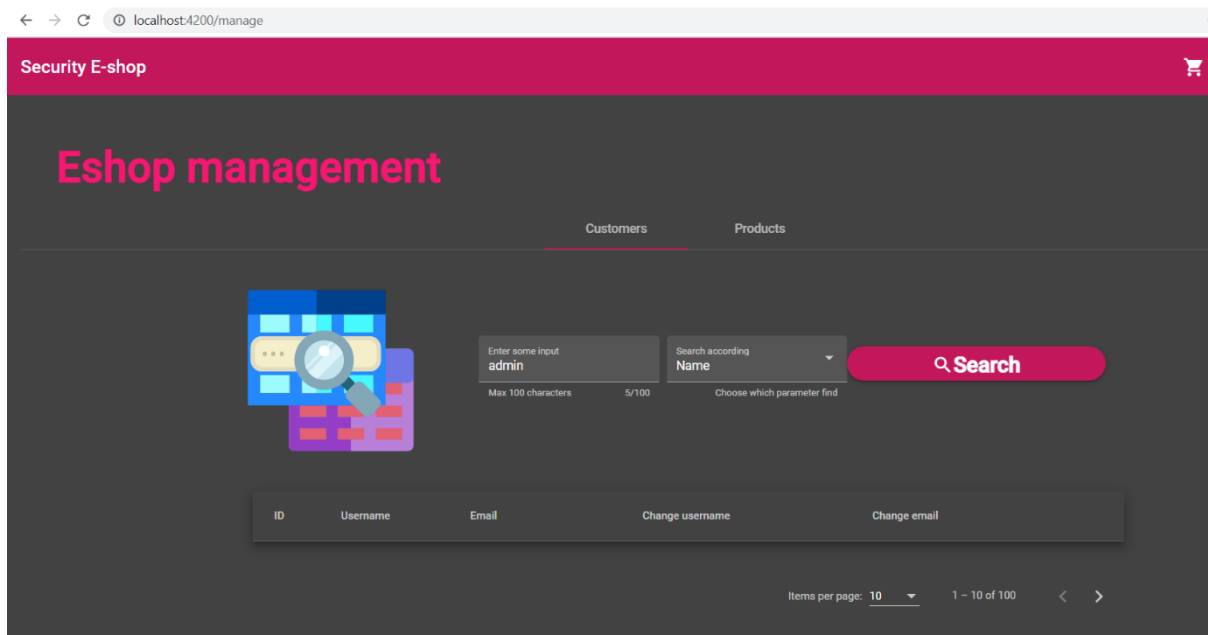
Útočník pri prelamaní hesiel sa bol schopný dostať do role pracovníka v obchode. Následne má prístup k používateľským emailom a menám. Jeho úlohou bude ale vyhľadať admina, ktorý sa nezobrazuje. Použije SQL injekciu. V tejto časti ponúkame postup pri scenári aplikovania SQL injekcie.

1. Kliknite na tlačidlo Board v pravom hornom rohu potom, čo ste prihlásený ako pracovník v obchode.



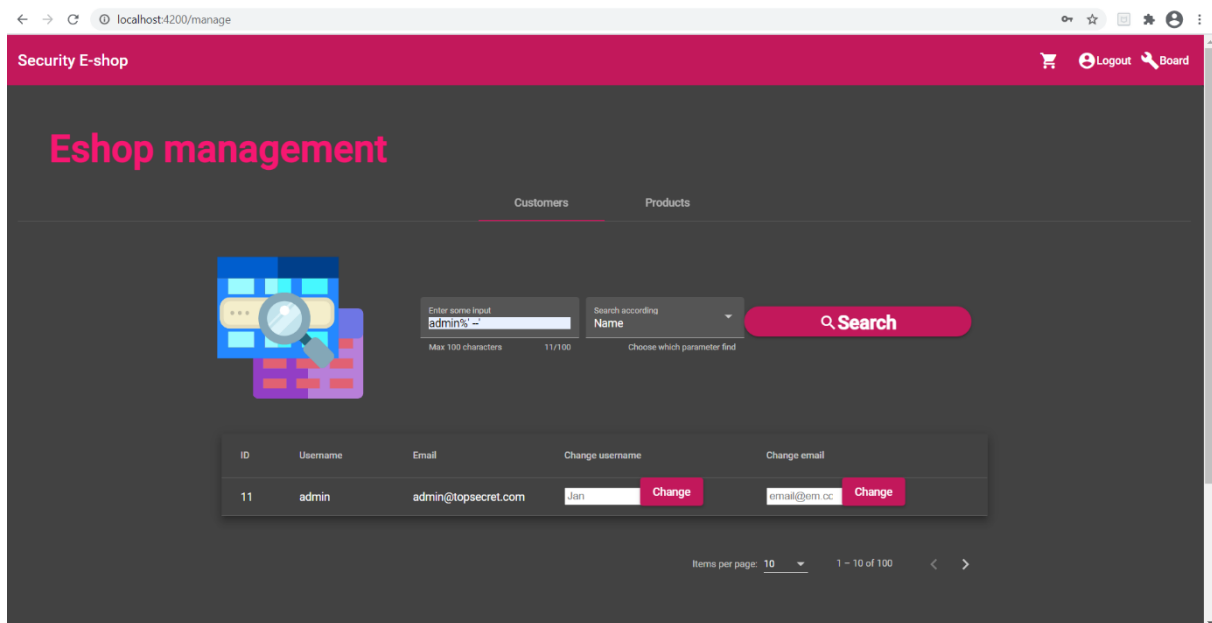
Obrázok 4: Pracovník v obchode má prístup k tabuli používateľov

2. V časti Customers sa pokúste vyhľadať používateľa s menom admin.



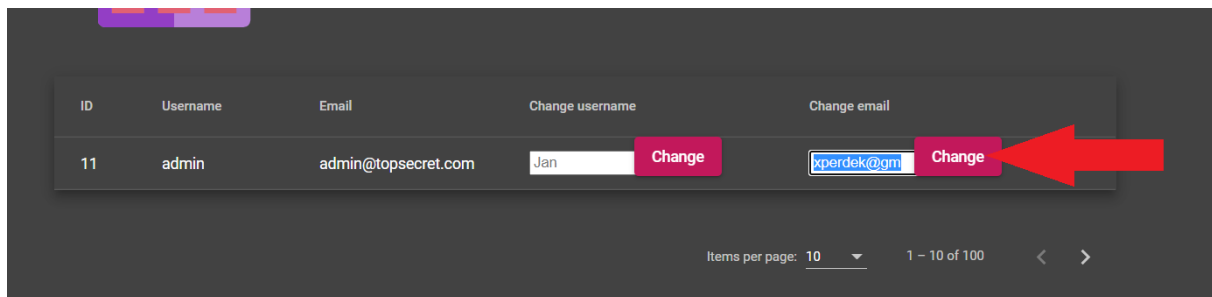
Obrázok 5: Pokus vyhľadať používateľa s menom admin

3. Skúste použiť SQL Injekciu pre používateľa admin, tým že necháte výraz admin vyhládať a zároveň odignorovať zvyšnú časť výrazu.



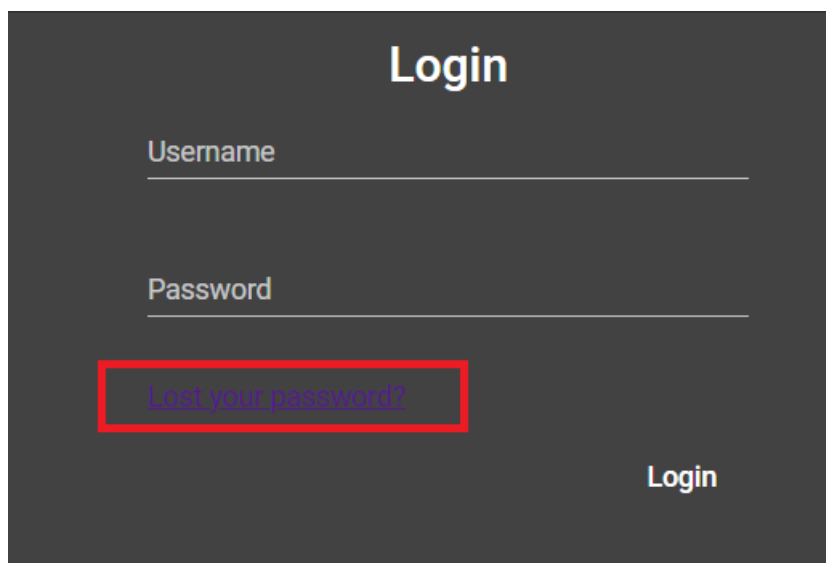
Obrázok 6: Použitie SQL Injekcie pre vyhľadanie používateľa s menom admin

4. Zmeňte email používateľa admin na svoj. Pre unikátnosť emailov nesmie byť tento email už predtým použitý.



Obrázok 7: Zmena emailovej adresy používateľa admin na svoj vlastný

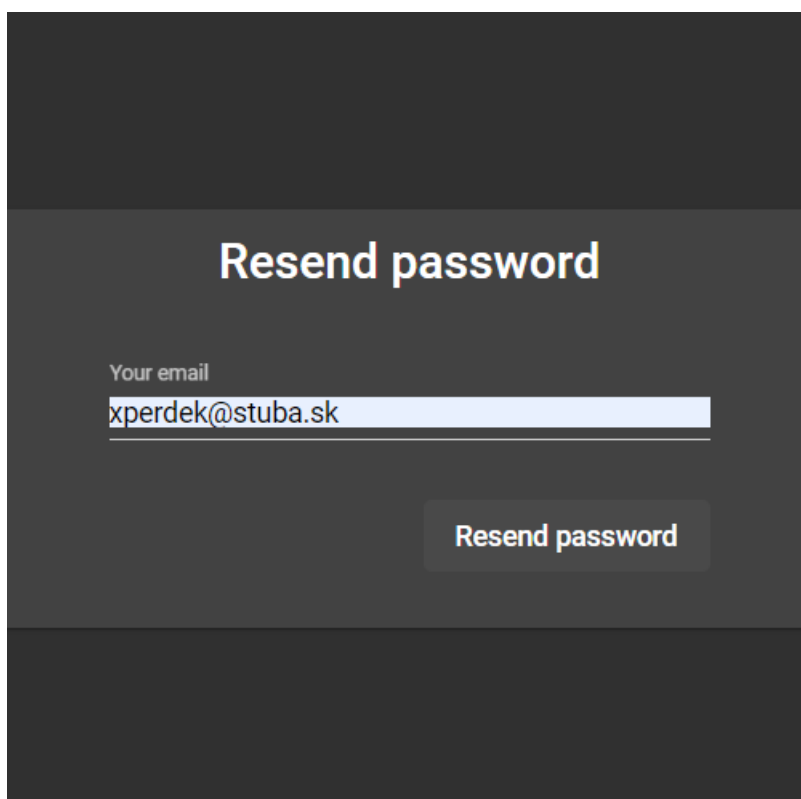
5. Odhláste sa kliknite na tlačidlo pre opätovné prihlásenie. Namiesto prihlásenia ale kliknite na odkaz Lost your password?



The image shows a dark-themed login form. At the top, the word "Login" is centered in a large, white, sans-serif font. Below it, there are two input fields: "Username" and "Password", both with white text labels and white underlines. Below the "Password" field, there is a link that says "Lost your password?" in a purple, underlined font. This link is enclosed in a red rectangular border. To the right of the "Lost your password?" link, there is a white "Login" button.

Obrázok 8: Prihlasovací formulár s odkazom na obnovu zabudnutého hesla

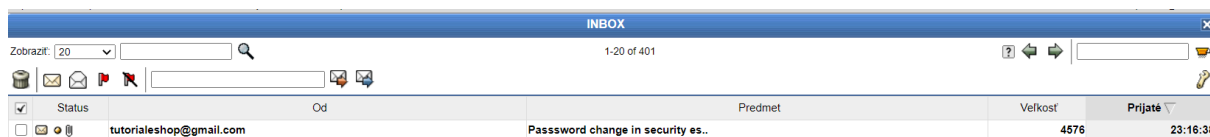
6. Na nasledujúcom formulári zadajte zmenený email a kliknite na tlačidlo Resend password.



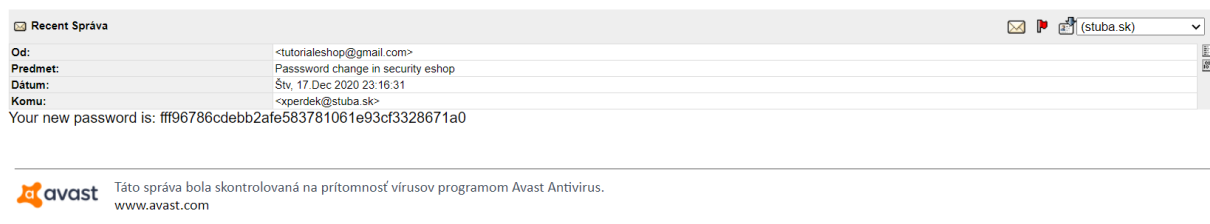
The image shows a dark-themed form for resetting a password. At the top, the text "Resend password" is centered in a large, white, sans-serif font. Below it, there is a label "Your email" in a small, white, sans-serif font. Underneath the label is an input field containing the email address "xperdek@stuba.sk" in a blue font. Below the input field, there is a white "Resend password" button.

Obrázok 9: Formulár pre pregenerovanie nového hesla

7. Otvorte svojho emailového klienta a počkajte kým vám príde email z eshopu. Potom z neho získajte heslo.



Obrázok 10: Doručenie správy so zmeneným heslom



Obrázok 11: Zmenené heslo sa nachádza v správe

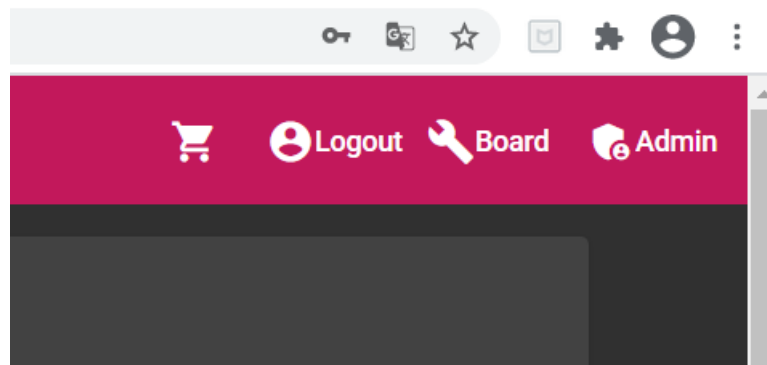
8. Prihláste sa pod menom admin a zadajte vygenerované heslo.

A screenshot of a login form on a dark background. The title 'Login' is centered at the top. Below it, there are two input fields: 'Username' with the text 'admin' and 'Password' with a masked password represented by dots. Below the password field, there is a link 'Lost your password?'. At the bottom right, there is a 'Login' button.

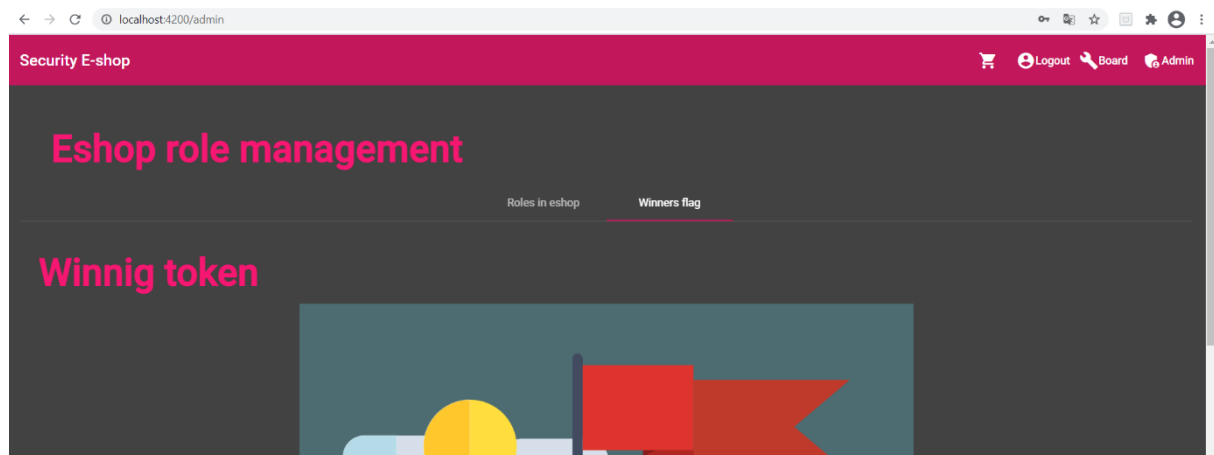
Obrázok 12: Vloženie zmenených údajov do formulára pre prihlásenie



9. Dostali ste sa do účtu, ktorý má najvyššie privilégium. Teraz môžete meniť privilégiá ostatných používateľov. Víťazný token/vlajku môžete nájsť v časti pre manažovanie rolí. Konečne je eshop dobytý!



Obrázok 13: Používateľ s privilégiom admin má vlastný ovládací panel

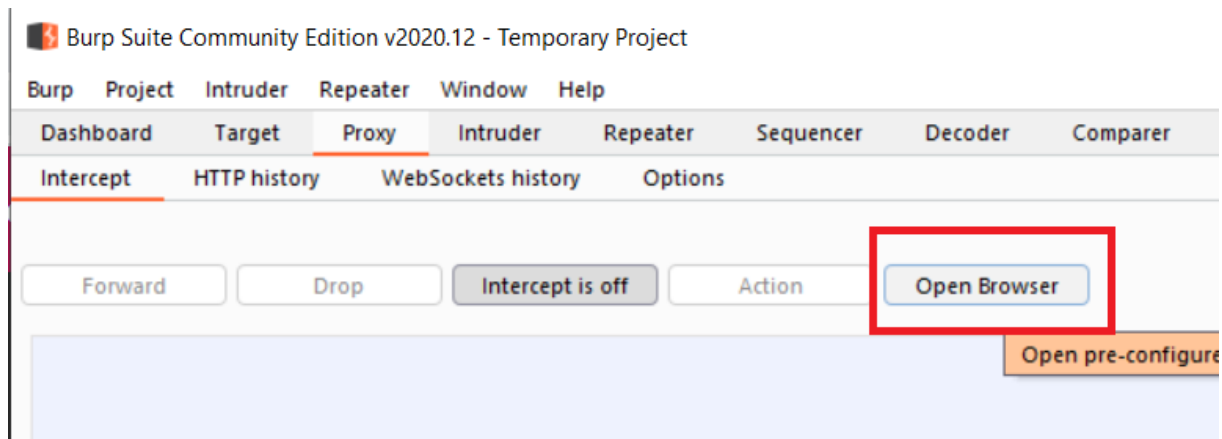


Obrázok 14: Prekliknutie sa na víťazný token

# Ukradnutie produktu z eshopu

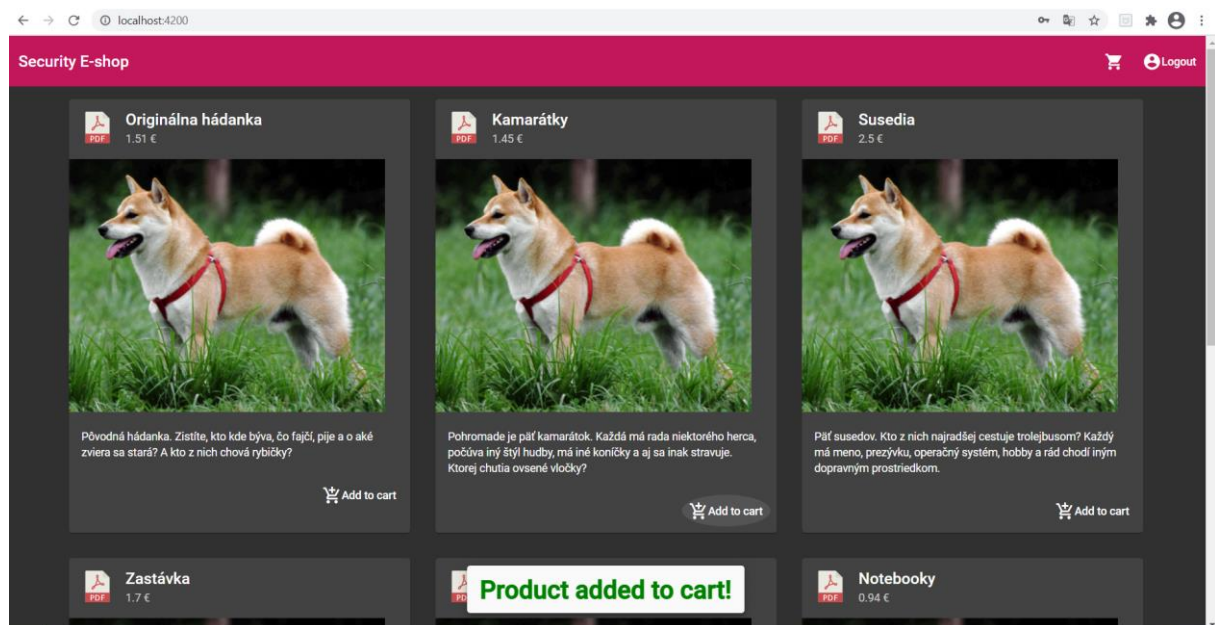
Útočník ukradne produkty z eshopu tým, že pošle vo formulári nulovú hodnotu. Najprv ale musí vytvoriť objednávku.

1. Otvorte program Burp Suite a prepnite sa na lištu Proxy. Následne otvorte prehliadač.



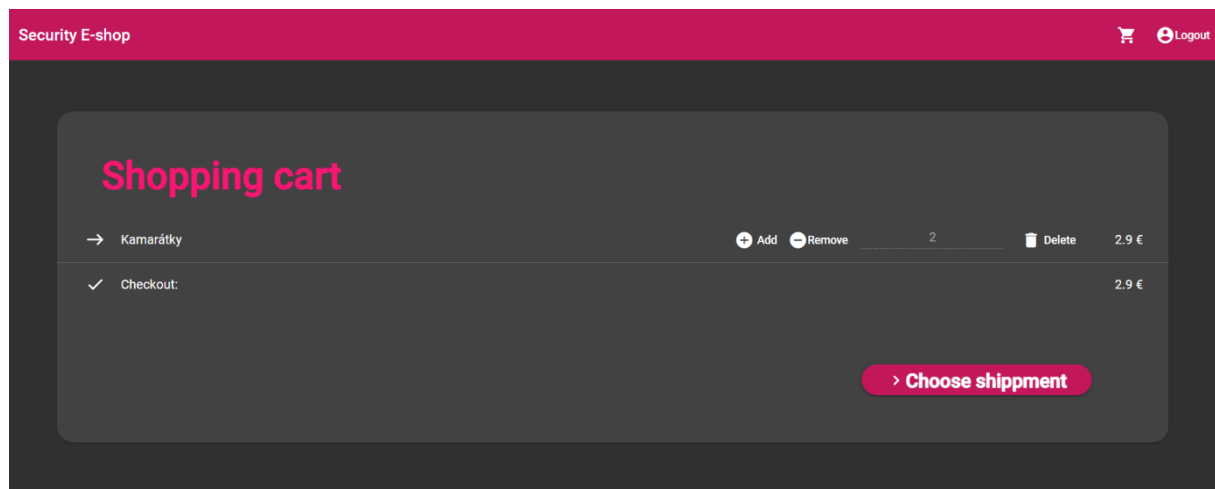
Obrázok 15: Zapnutie burpsuite a otvorenie vlastného prehliadača

2. Prihláste sa pod ľubovoľným používateľom a pridajte nejaký produkt do košíka.



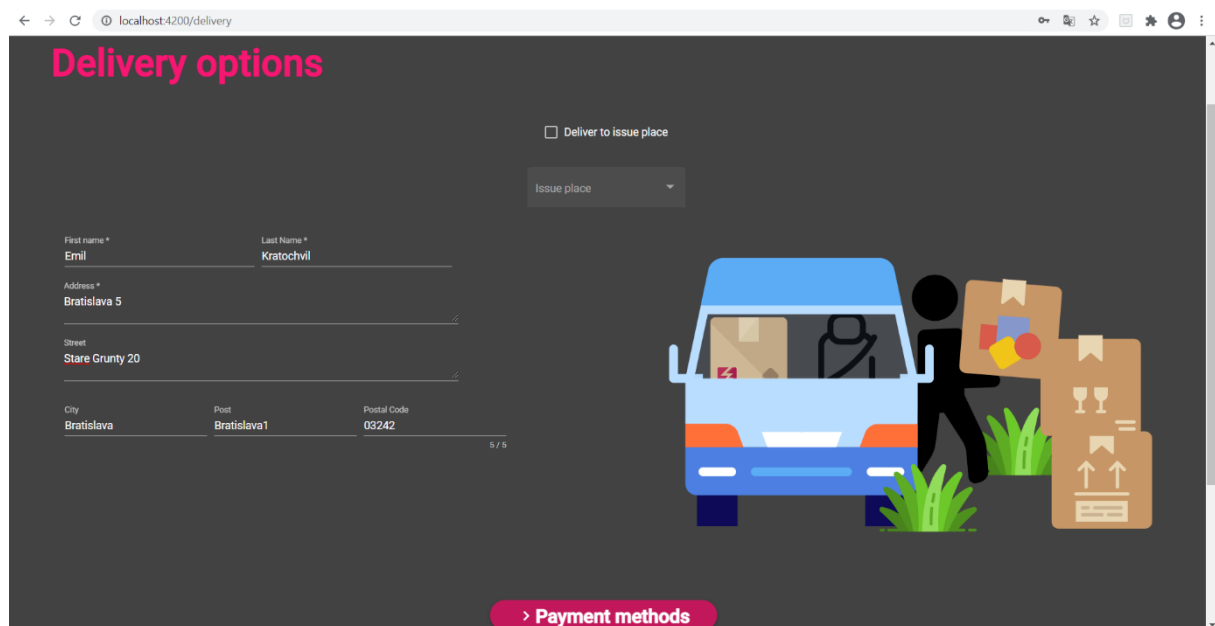
Obrázok 16: Pridanie produktu do košíka

3. Potvrďte produkty v košíku vybraním výberu spôsobu dodania stlačením na tlačidlo Choose shippment.



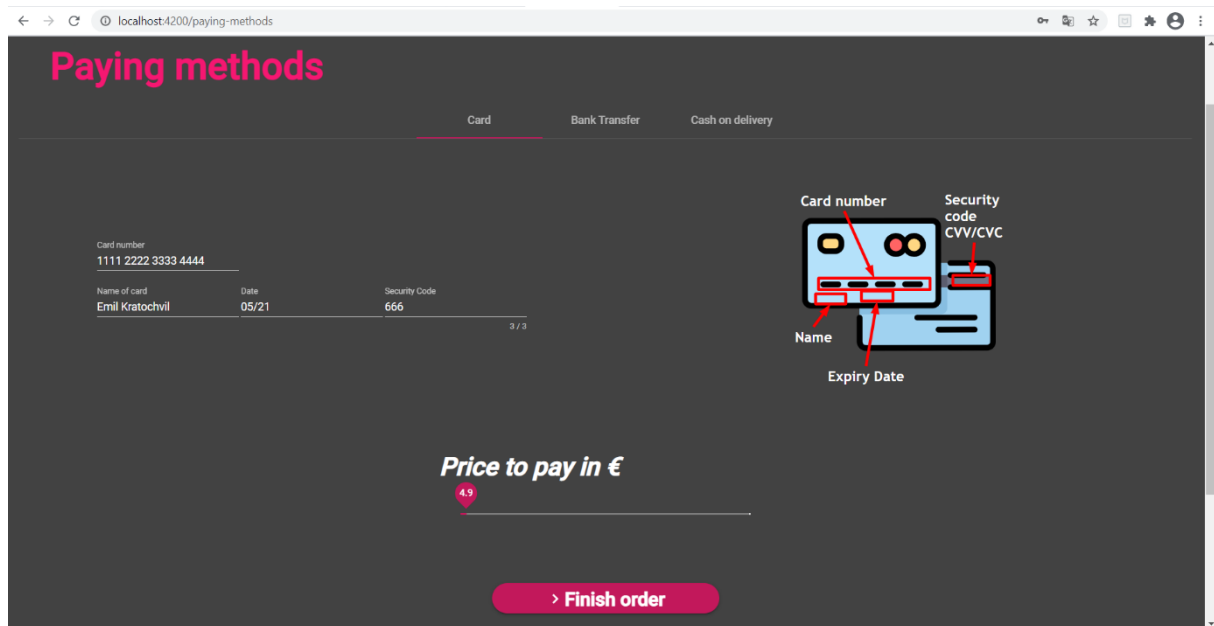
Obrázok 17: Potvrdenie produktov v košíku

4. Zadaťte informácie o dodaní. Nejakú adresu a ďalšie potrebné údaje a potvrďte.



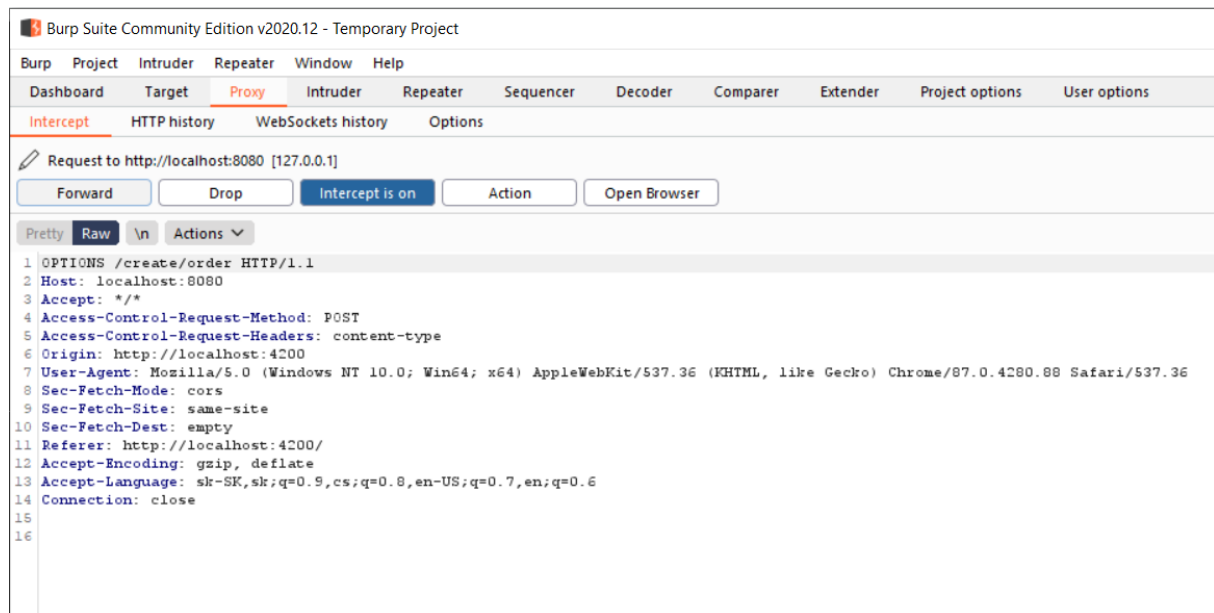
Obrázok 18: Určenie dodacej adresy

5. Vyberte nejakú platobnú metódu. Pred potvrdením nezabudnite v Burp Suite zapnúť intercept na on. Následne potvrdíte.



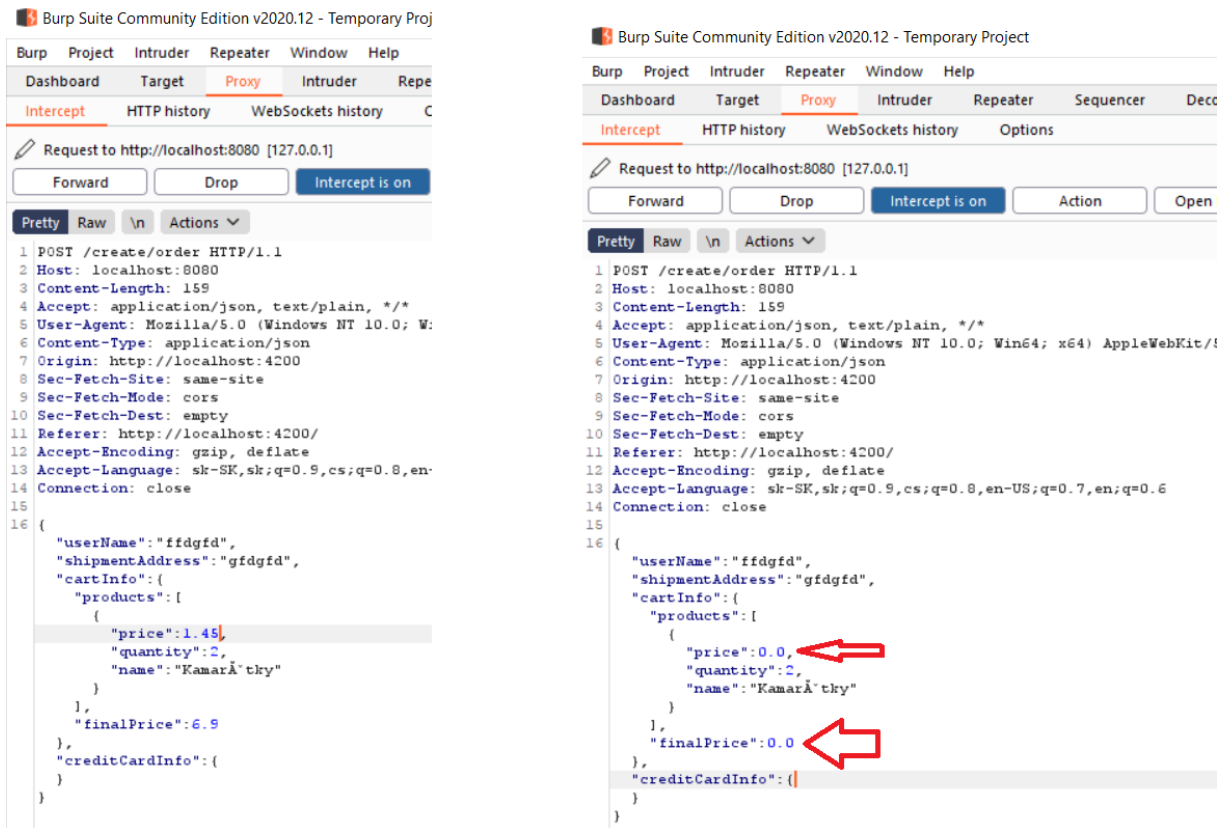
Obrázok 19: Zadanie informácií o platbe a potvrdenie

6. Prvý request prepošlite stlačením tlačidla forward.



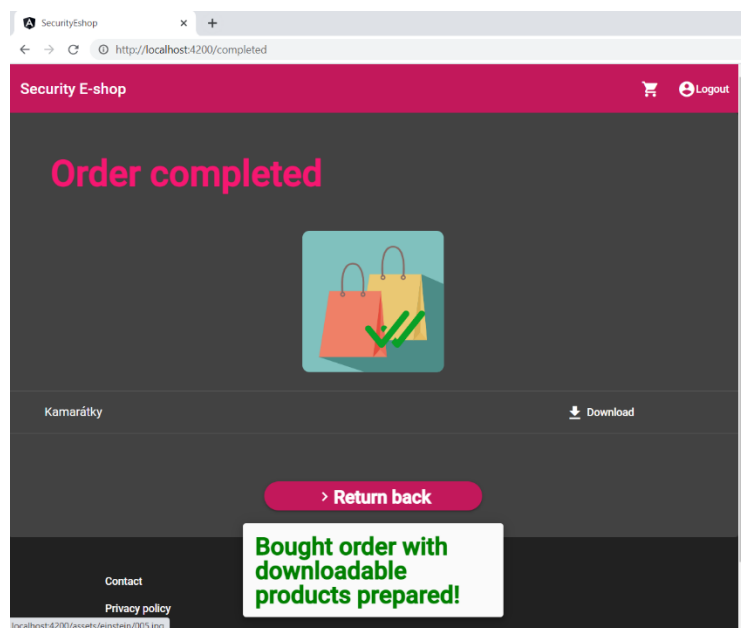
Obrázok 20: Ignorovanie prvého requestu

7. V druhom requeste zmeníte finalPrice na 0. Pre istotu zmeníte aj všetky ceny produktov na nulu. Následne stlačíte forward.



Obrázok 21: Zmena informácií v druhom requeste

8. Objednávka bola úspešne uskutočnená. Teraz si môžete stiahnuť ukradnuté produkty.

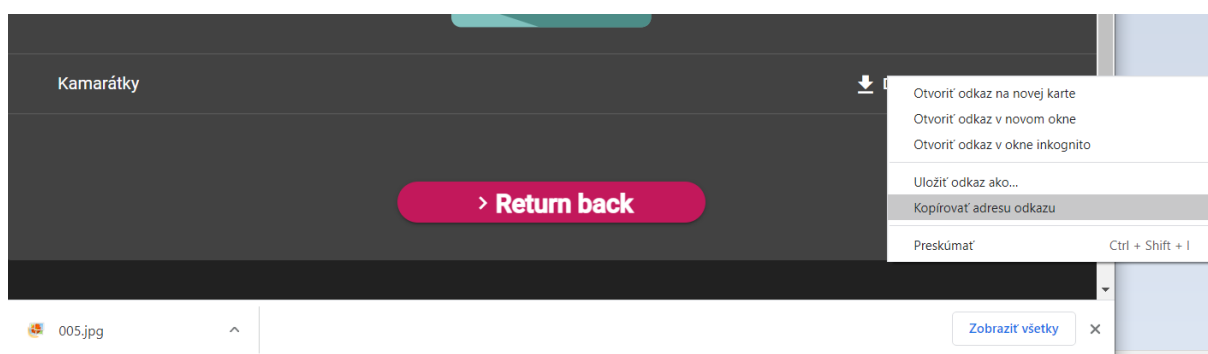


Obrázok 22: Stiahnutie ukradnutých produktov

# Získanie prístupu k súborom

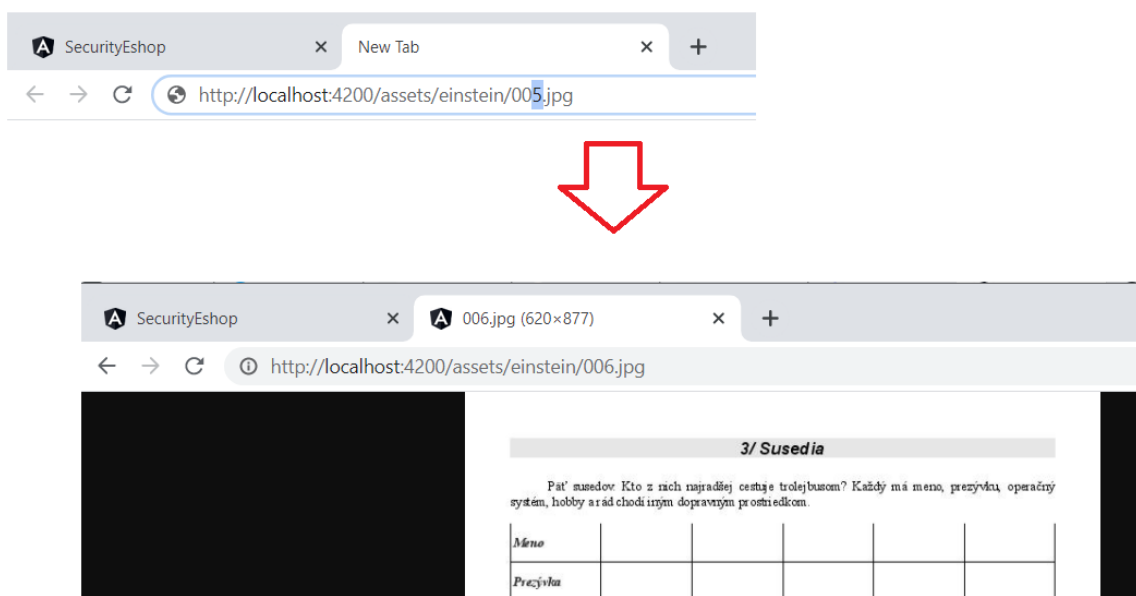
Útočník by mal vedieť, že ako technológia bol použitý Angular. Na základe tejto informácie by mal byť schopný dostať sa k verejne uloženým súborom na stránke zadáním do prehliadača cestu k assets/images. Už je len potrebné zistiť presnú cestu. Pri minulom scenári s ukradnutím produktu si ale môže všimnúť, že produkty obsahujú cestu vedúcu na frontend a verejne dostupnú. Inkrementuje číslo nejakého súboru a získa ďalší zo súborov bez väčšej námahy. Následne môže stiahnuť obsah ponúkaných produktov aj bez nutnosti platby za ne.

1. Získajte odkaz z ukradnutého súboru.



Obrázok 23: Získanie odkazu na stiahnutý obsah

2. Použite podobný názov súboru pri zadaní do okna prehliadača.



Obrázok 24: Vyskúšanie podobnej adresy s inkrementovaným číslom obrázka