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

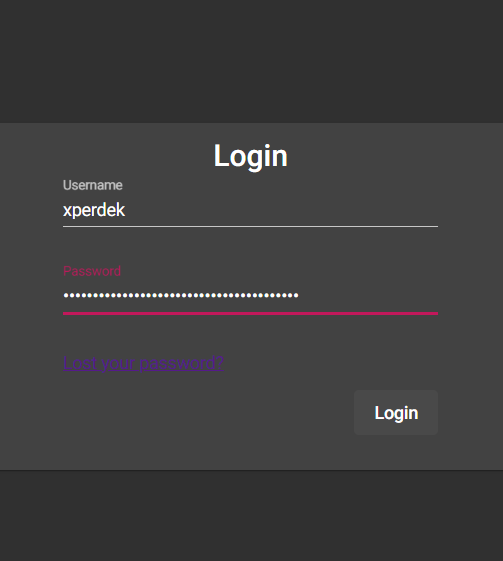
Na začiatku sa používateľ zaregistruje. Vyplní všetky položky registračného formulára. Zapamätá si meno a heslo a uvedie funkčný a jedinečný email. Následne použije meno a heslo pri prihlasovaní. Automaticky mu bude priradená roľa používateľa.

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

# 

Obrázok 1: Registrácia používateľa

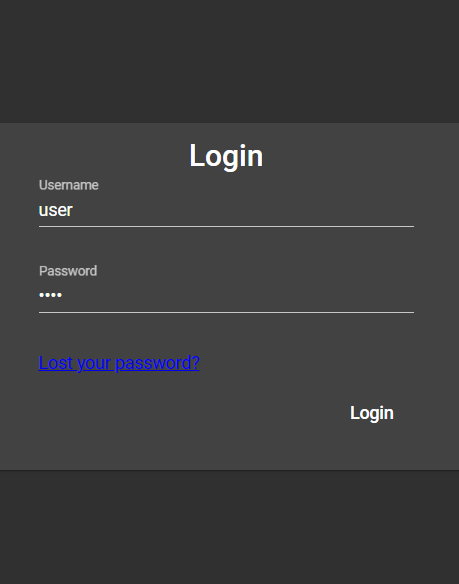
1. Následne sa prihláste zadaním vášho používateľského mena a hesla.



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 Angulár. Stačí ak vyskúša jednoduché heslá ručne. Rovnako si môže zistiť hash hesla vytvorený bcryp-tom vrátený do Anguláru 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 najpoužívanejších hesiel.

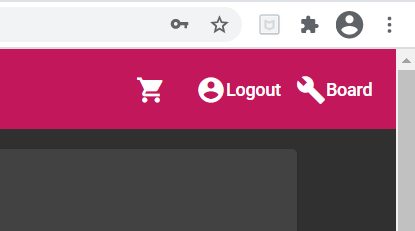


Obrázok 3: Aplikovanie jednoduchého hesla user

# Použitie SQL injekcie

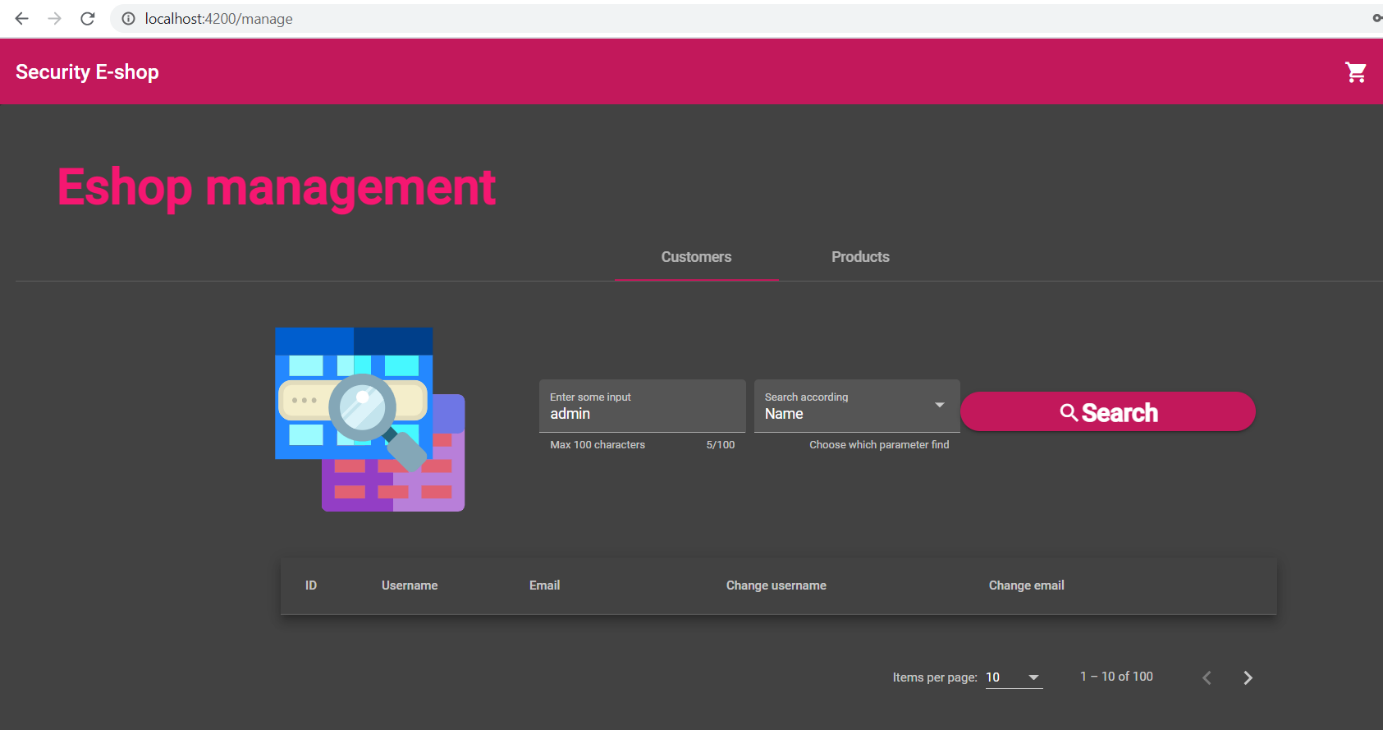
Útočník pri prelamovaní hesiel sa bol schopný dostať do role pracovníka v obchode. Následne má prístup k používateľským emailom a menám. Jeho úlohou bude ale vyhľadať admina, ktorý sa nezobrazuje. Použije SQL injekciu. V tejto časti ponúkame postup pri scenári aplikovania SQL injekcie.

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



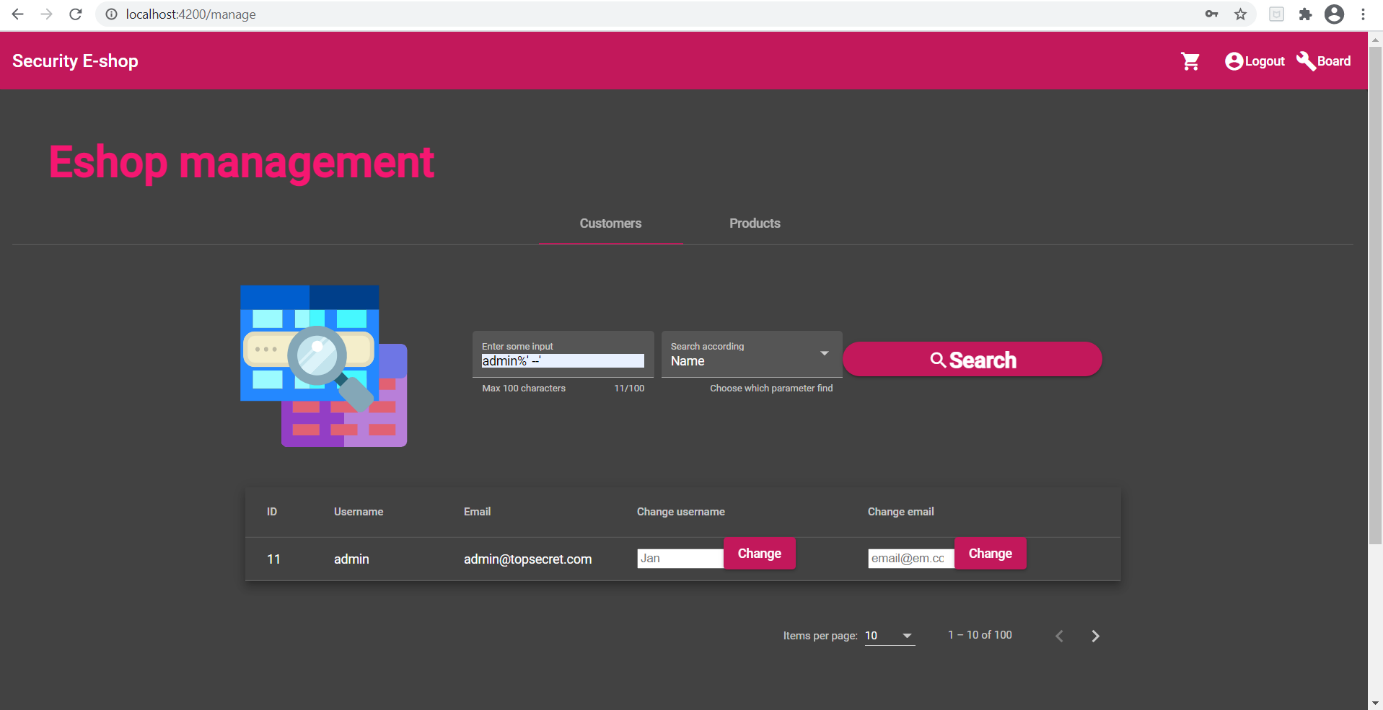
Obrázok 4: Pracovník v obchode má prístup k tabuli používateľov

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



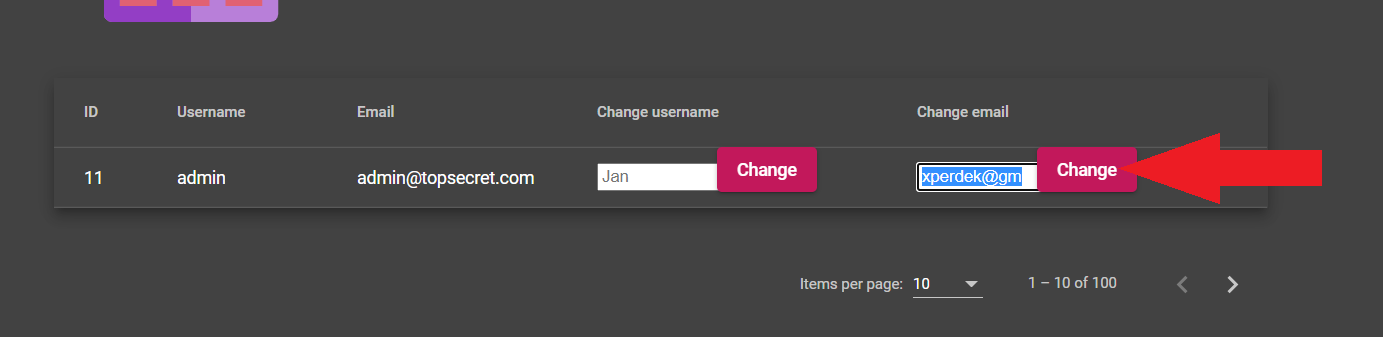
Obrázok 5: Pokus vyhľadať používateľa s menom admin

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



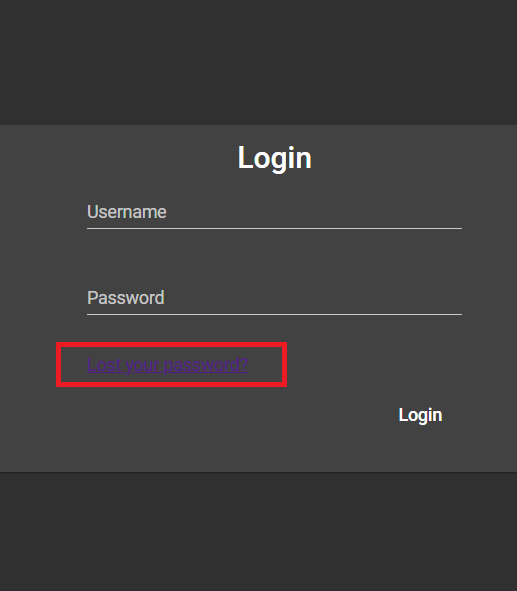
Obrázok 6: Použitie SQL Injekcie pre vyhľadanie používateľa s menom admin

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



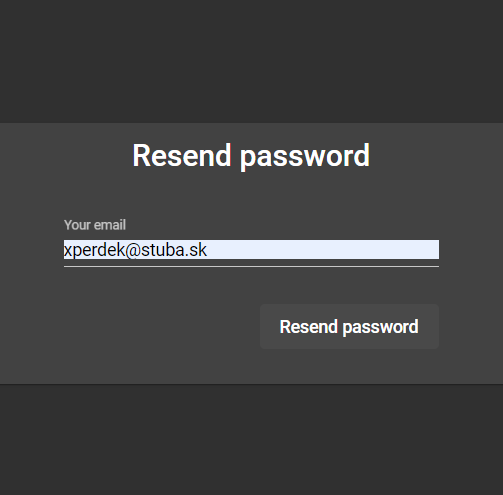
Obrázok 7: Zmena emailovej adresy používateľa admin na svoj vlastný

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



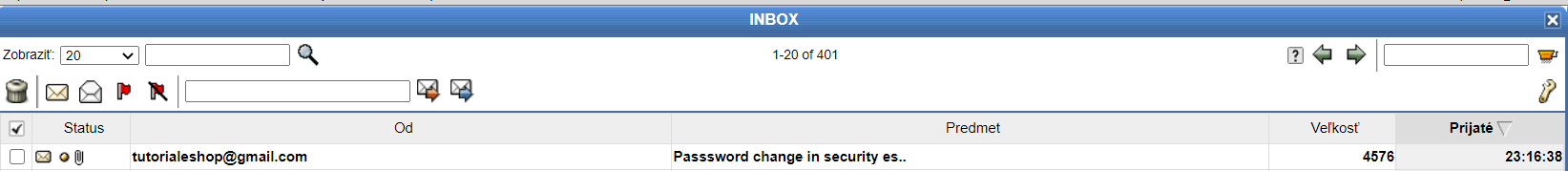
Obrázok 8: Prihlasovací formulár s odkazom na obnovu zabudnutého hesla

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

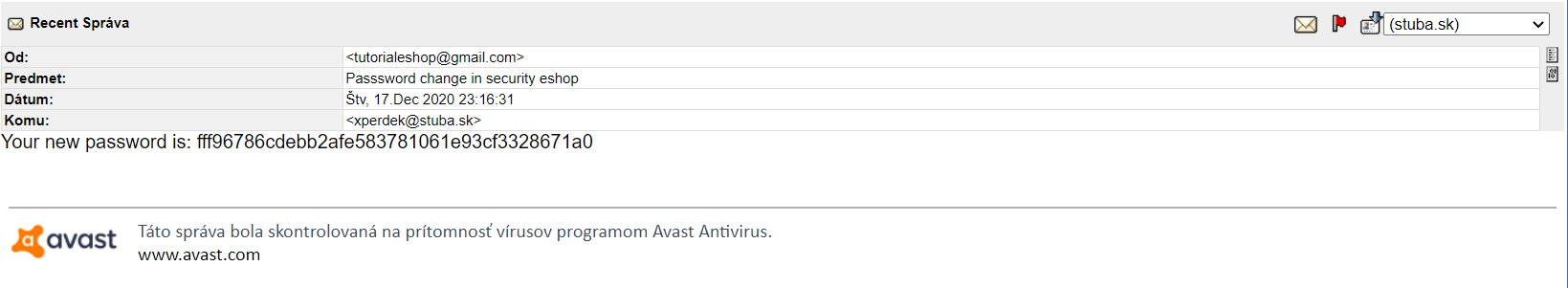


Obrázok 9: Formulár pre pregenerovanie nového hesla

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

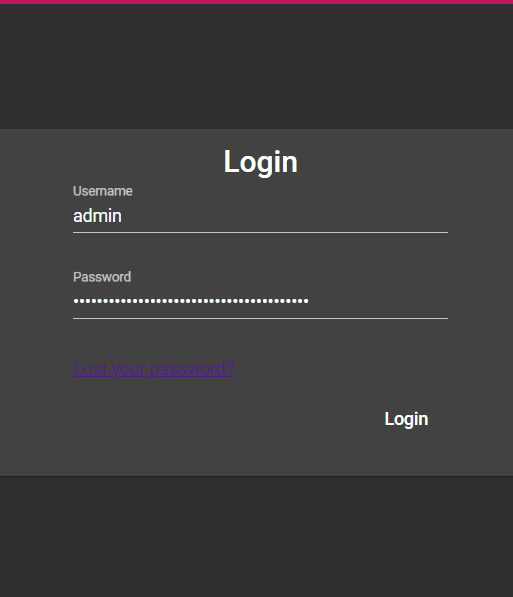


Obrázok 10: Doručenie správy so zmeneným heslom



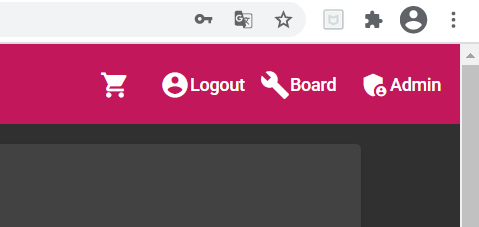
Obrázok 11: Zmenené heslo sa nachádza v správe

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

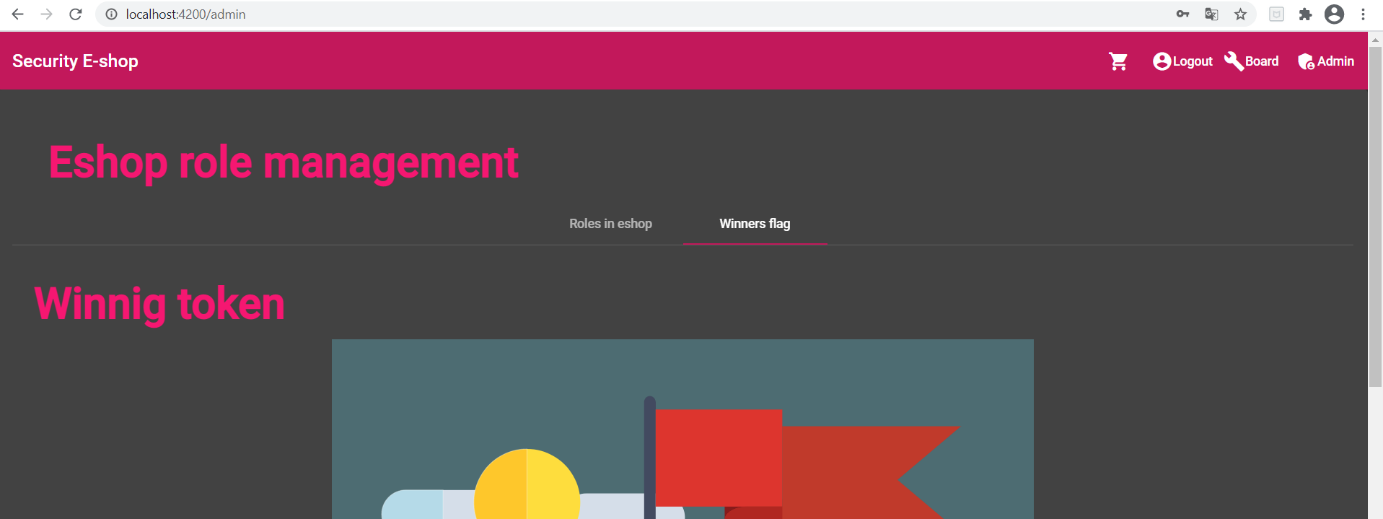


Obrázok 12: Vloženie zmenených údajov do formulára pre prihlásenie

1. 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

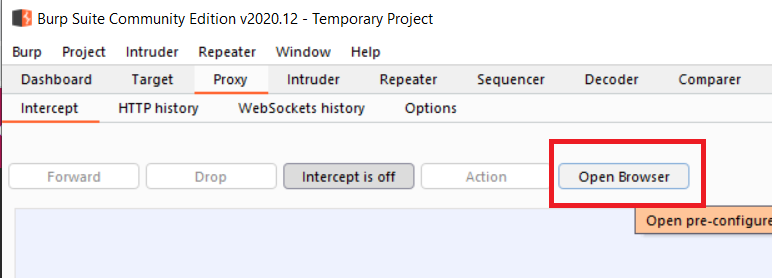


Obrázok 14: Prekliknutie sa na víťazný token

# Ukradnutie produktu z eshopu

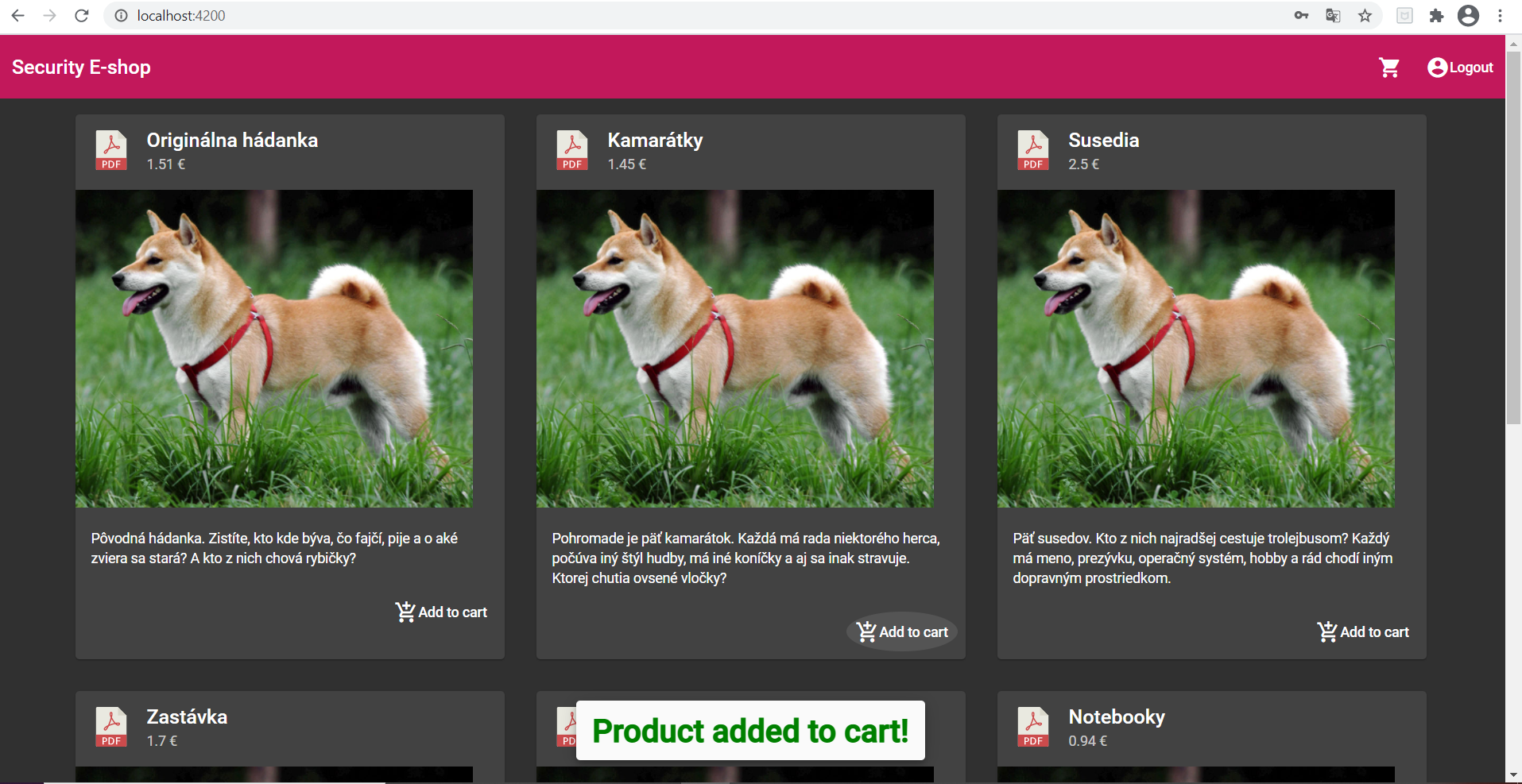
Útočník ukradne produkty z eshopu tým, že pošle vo formulári nulovú hodnotu. Najprv ale musí vytvoriť objednávku.

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



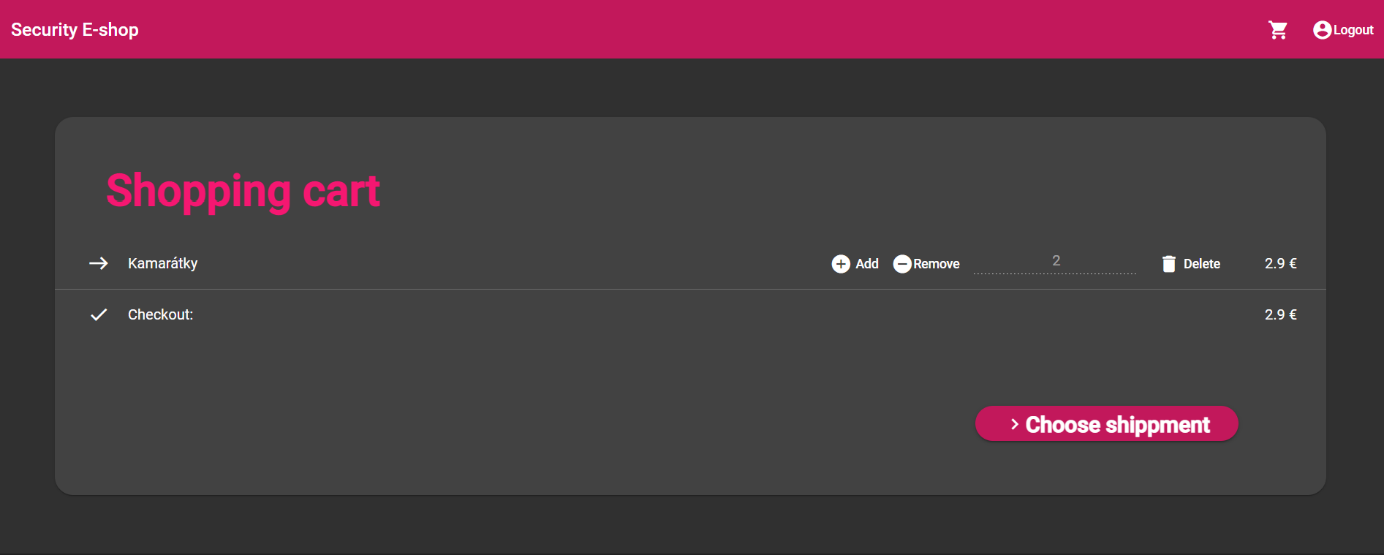
Obrázok 15: Zapnutie burpsuite a otvorenie vlastného prehliadača

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



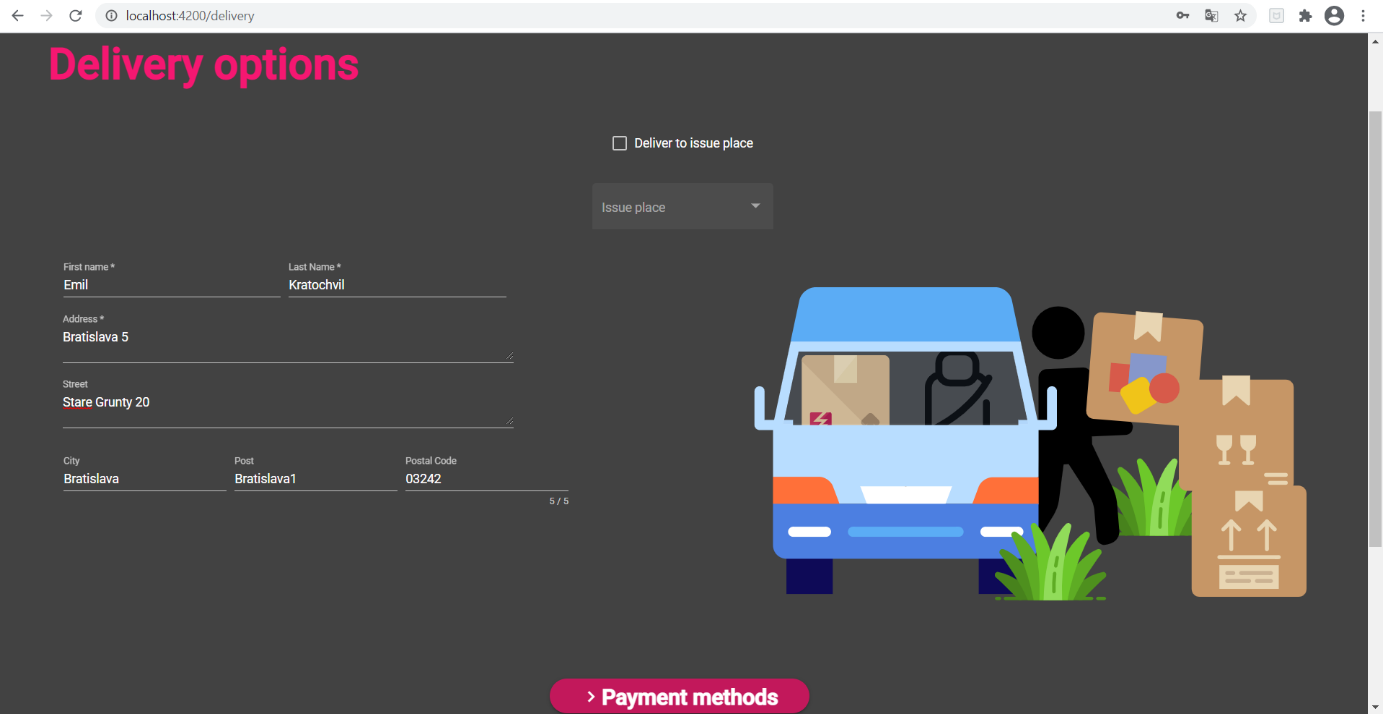
Obrázok 16: Pridanie produktu do košíka

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



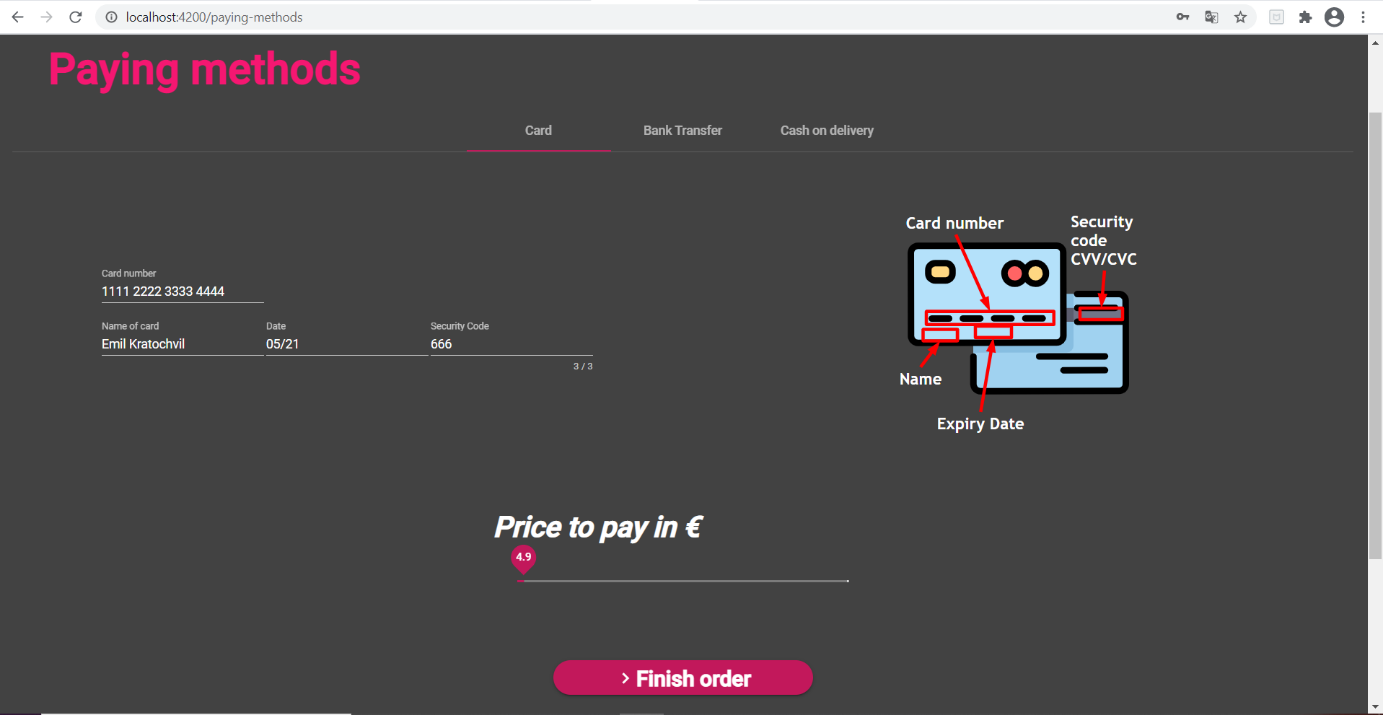
Obrázok 17: Potvrdenie produktov v košíku

1. Zadajte informácie o dodaní. Nejakú adresu a ďalšie potrebné údaje a potvrďte.



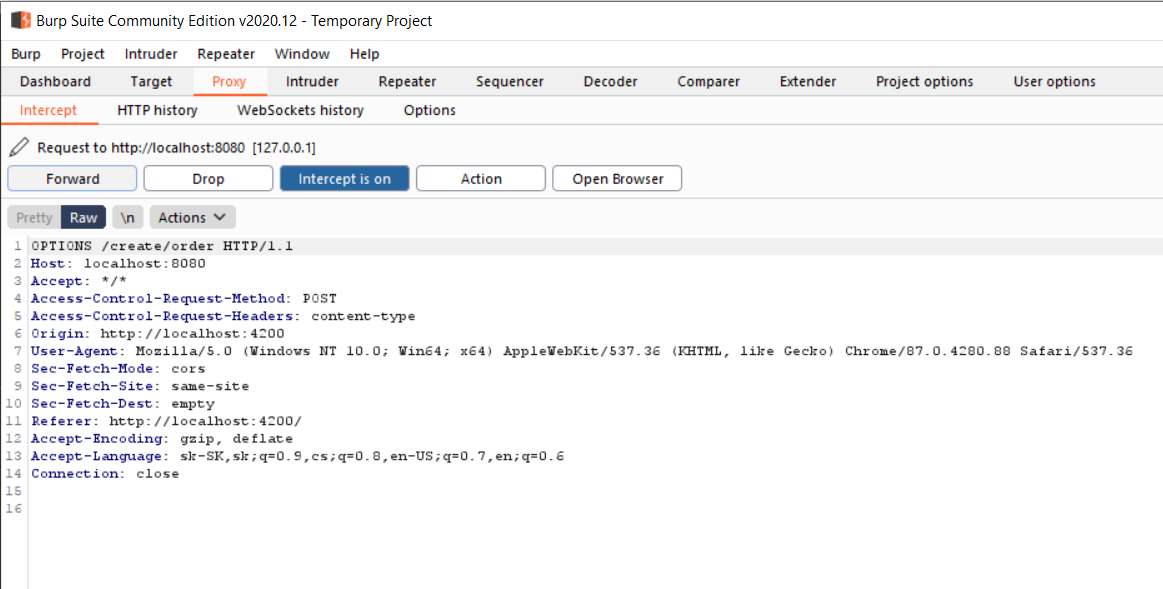
Obrázok 18: Určenie dodacej adresy

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



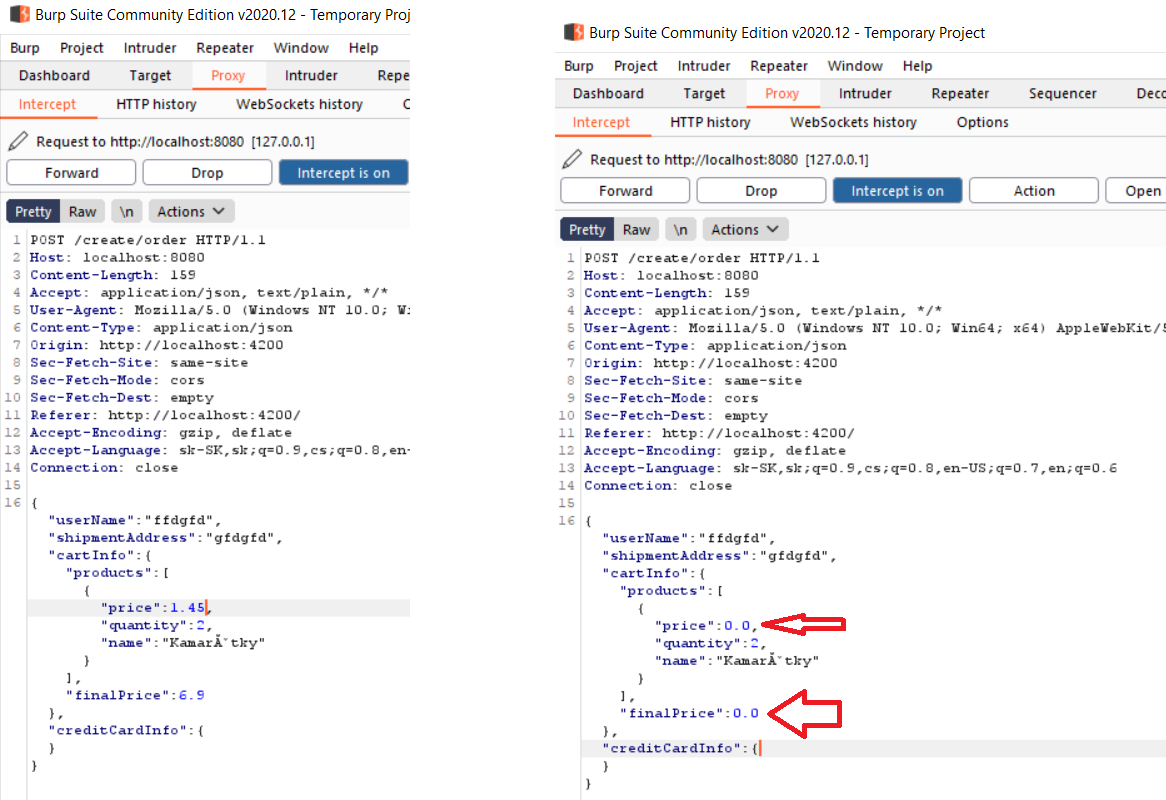
Obrázok 19: Zadanie informácií o platbe a potvrdenie

1. Prvý request prepošlite stlačením tlačidla forward.



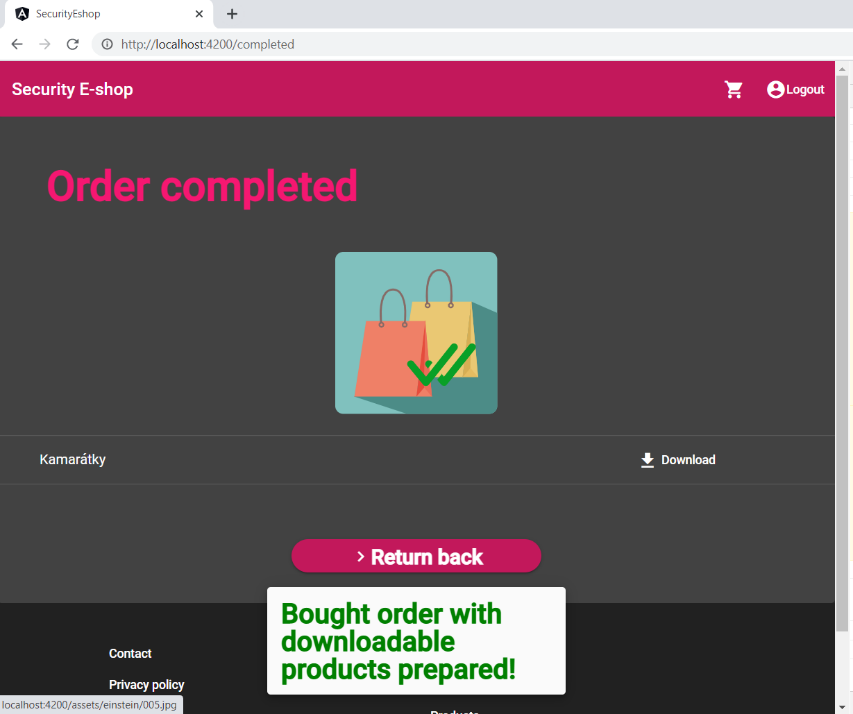
Obrázok 20: Ignorovanie prvého requestu

1. V druhom requeste zmeňte finalPrice na 0. Pre istotu zmeňte aj všetky ceny produktov na nulu. Následne stlačte forward.



Obrázok 21: Zmena informácií v druhom requeste

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

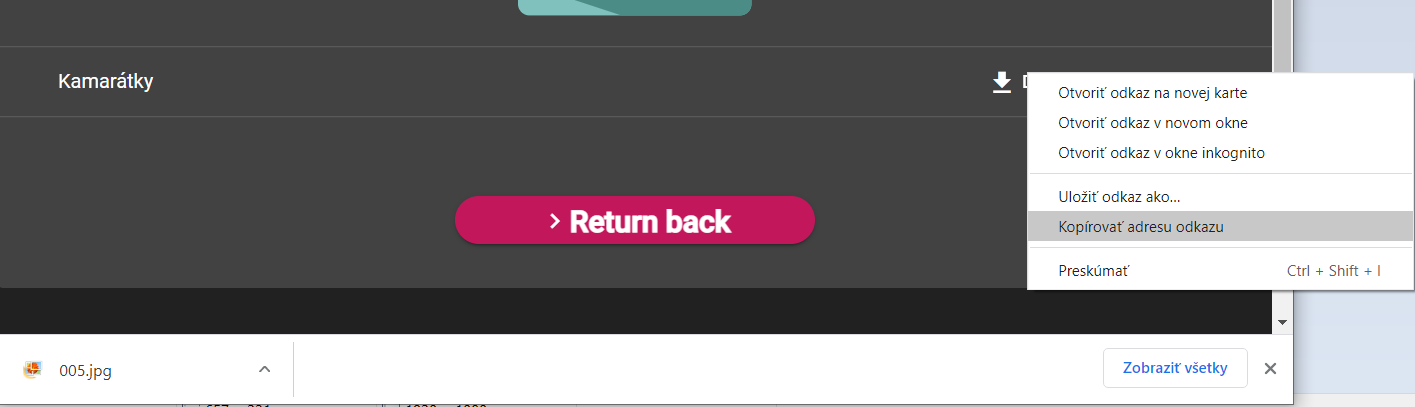


Obrázok 22: Stiahnutie ukradnutých produktov

# Získanie prístupu k súborom

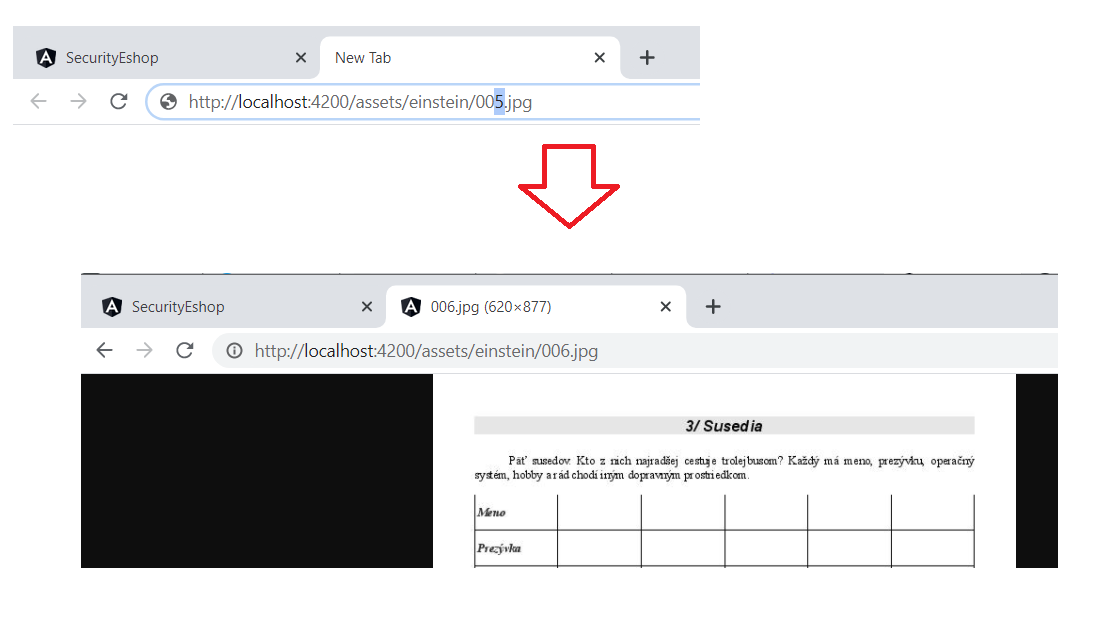
Útočník by mal vedieť, že ako technológia bol použitý Angulár. Na základe tejto informácie by mal byť schopný dostať sa k verejne uloženým súborom na stránke zadaním do prehliadača cestu k assets/images. Už je len potrebné zistiť presnú cestu. Pri minulom scenári s ukradnutím produktu si ale môže všimnúť, 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

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



Obrázok 24: Vyskúšanie podobnej adresy s inkrementovaným číslom obrázka