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

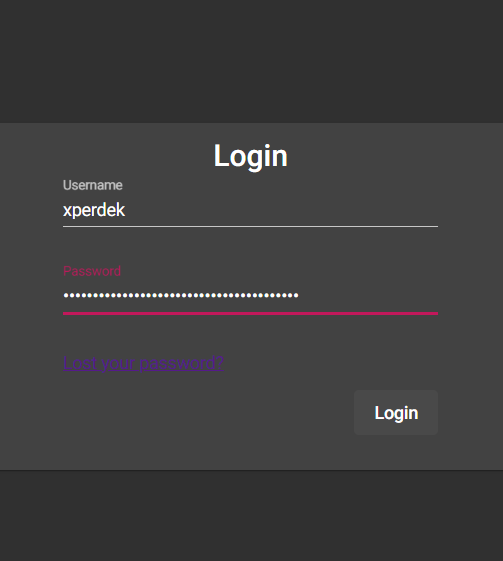
Na začiatku sa používateľ zaregistruje. Vyplní všetky položky registračného formulára. Zapamätá si meno a heslo a uvedie funkčný a jedinečný email. Následne použije meno a heslo pri prihlasovaní. Automaticky mu bude priradená roľa používateľa.

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

# 

Obrázok 1: Registrácia používateľa

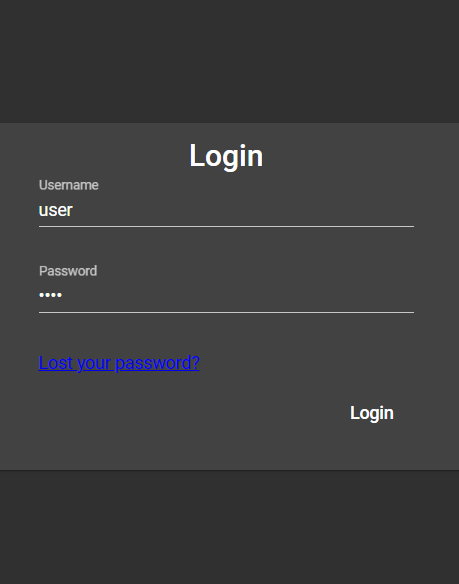
1. Následne sa prihláste zadaním vášho používateľského mena a hesla.



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.

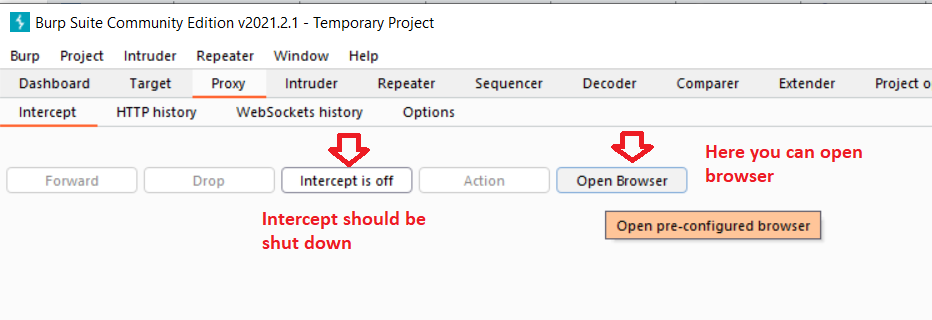


Obrázok 3: Aplikovanie jednoduchého hesla user

# Prelamovanie hesiel slovníkovým útokom

Útočník môže zrealizovať slovníkový útok na základe získaných informácií z login stránky. K užitočným informáciám sa dostanete na základe nasledujúceho postupu:

1. Po zapnutí burpsuitu a prejdite do kolónky proxy.
2. Vypnite intercept v rozkliknutom menu BurpSuite.
3. Otvorte si prehliadač kliknutím na open browser.



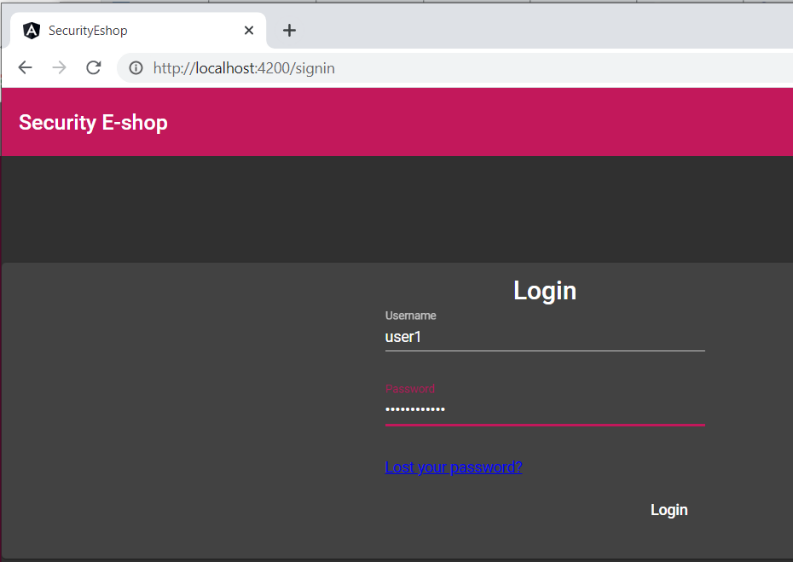
Obrázok 4: Otvorenie prehliadača a interceptor v BurpSuite

1. Prejdite na stránku <http://localhost:4200/signin>.
2. Zapnite intercept na tej istej položke v menu BurpSuite.



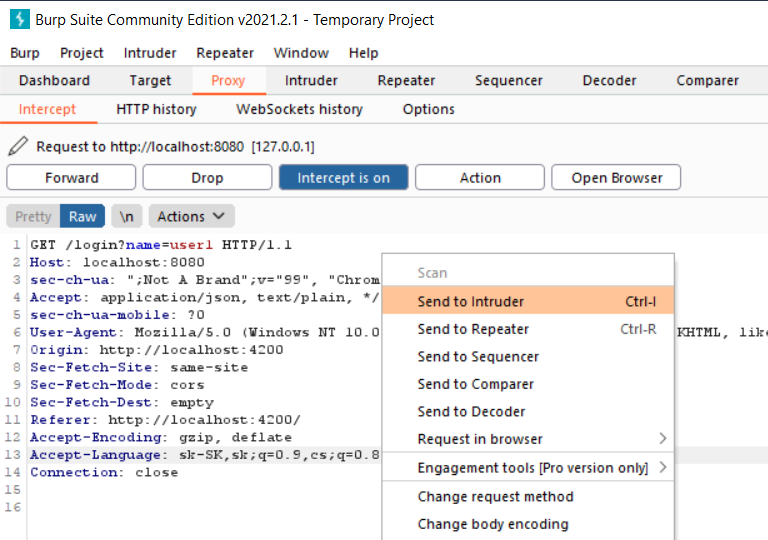
Obrázok 5: Zapnutie interceptora

1. Pokúste sa prihlásiť s ľubovoľným menom a heslom.



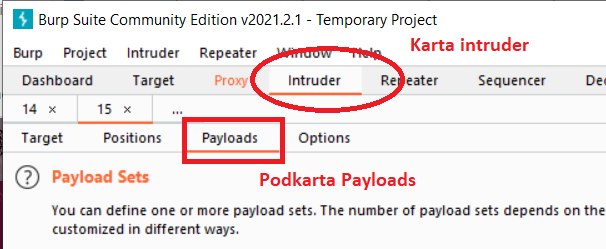
Obrázok 6: Pokus o prihlásenie v stavanom prehlaidači BurpSuitu

1. Následne sa prepnite do burpsuitu, kde sa zobrazí informácia o dopyte,
2. Zobrazte menu kliknutím ľavým tlačidlom myši do prostriedku informácií o dopyte.
3. Z menu vyberte položku “Send to Intruder”.

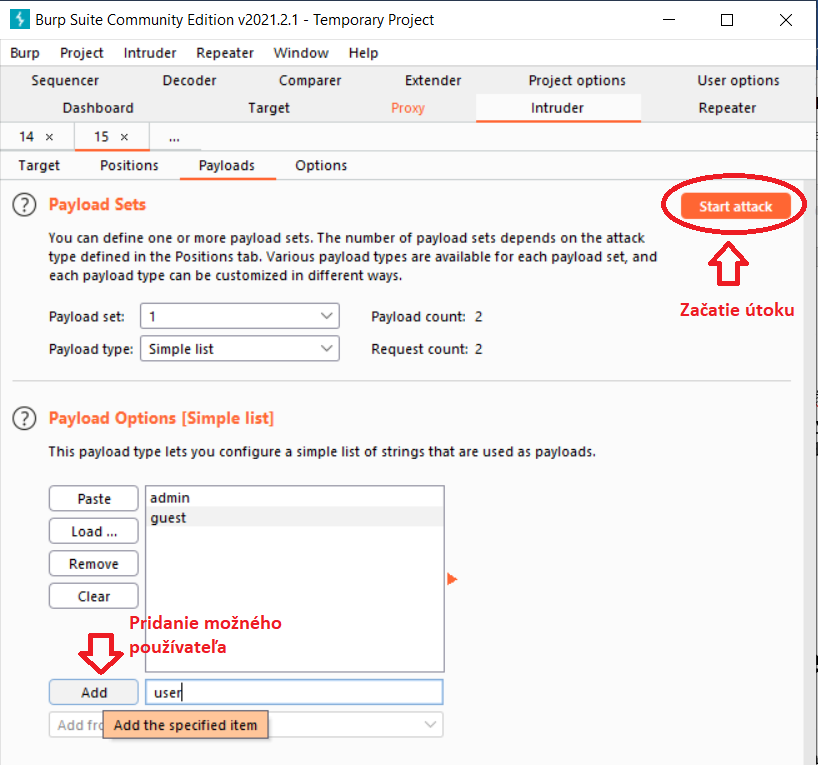


Obrázok 7: Odoslanie requestu do intrudera

1. Následne kliknite na otvorenú položku Intruder-a.
2. Rozkliknite podmenu Payloads v položke Intruder-a.

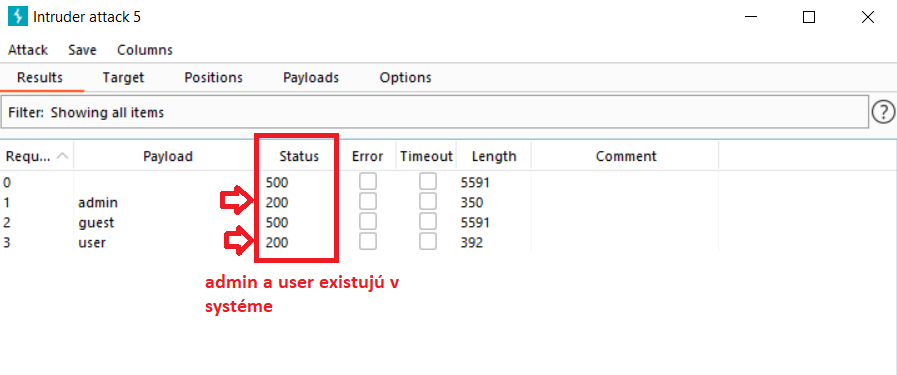


1. Obrázok 8: Presunutie sa na položku Payloads v Intruderovi
2. Vo vrchnej časti Payload Sets rozkliknutej karty v BurpSuite nechajte nastavené Payload set na 1 a Payload type na Simple list.
3. Nižšie v rozkliknutej karte nájdite časť Payload options a pomocou tlačítka Add pridajte niekoľko mien, ktoré by mohli byť potencionálni používatelia, pričom sa riadte častými názvami ako admin, user, guest a podobne.
4. Zvoľte položku “Start attack”.



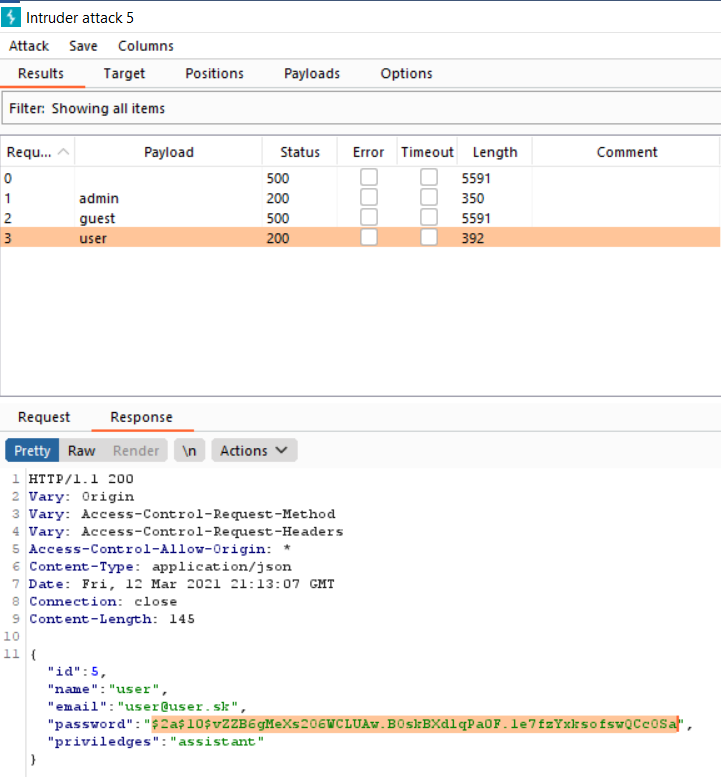
Obrázok 9: Zadanie zoznamu potencionálnych používateľov a začatie útoku

1. Otvorí sa okno, v ktorom podľa vráteného statusu môžte zistíť, ktorí používatelia existujú v systéme.
2. Kliknite na jeden z riadkov, ktorý má status 200.
3. Prepnite sa na kartu Response, v okne ktoré sa zobrazí nižšie.
4. Môžte zistiť, že aplikácia dostala heslo spolu s emalom a roľou používateľa. Pre admina zistíte, že jeho heslo nie je zahešované. Naopak pre používateľa zistíte, že jeho heslo je hash. Systém teda heslá šifruje, inak by sme sa prihlásili pomocou získaného hesla. Účet admina bude nejak zablokovaný. So získaných informácií zistíte, že používateľ user je v skutočnosti asistent. Skúsime preto v nasledujúcej časti zistiť jeho heslo.



Obrázok 10: Zistenie existujúcich používateľov v systéme

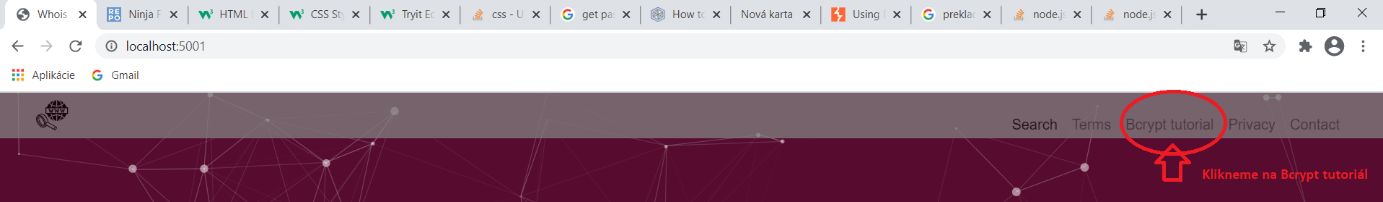
1. Skopírujte heslo usera, ktorý je asistent.



Obrázok 11: Získanie zašifrovaného hesla asistenta s používateľským menom user

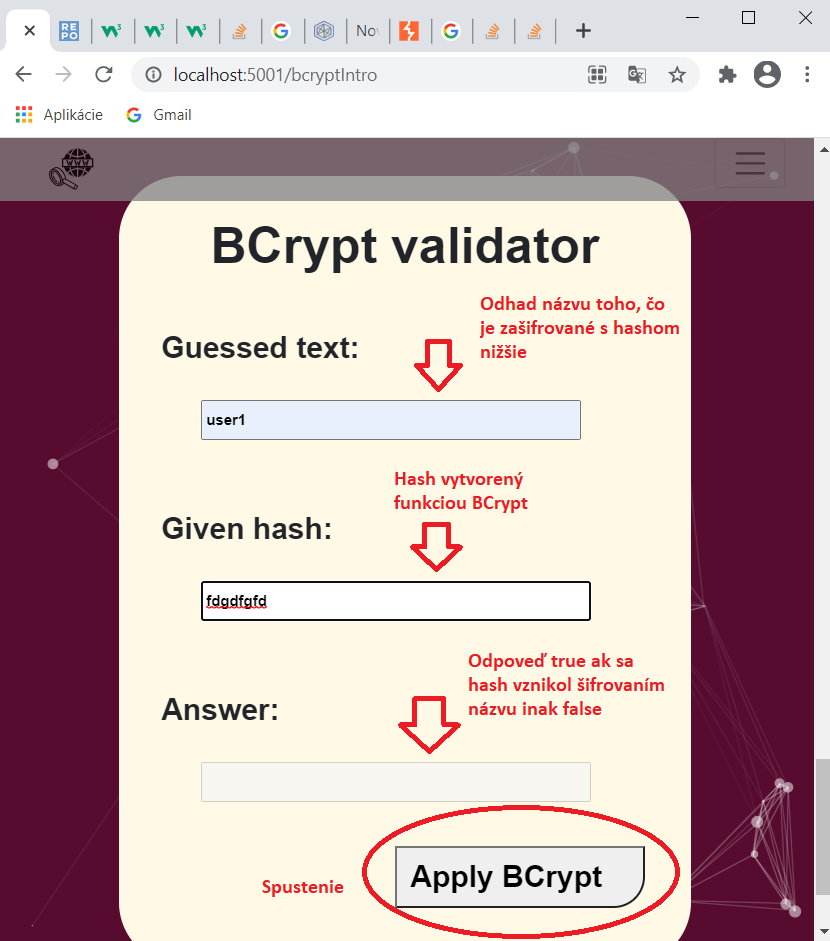
Získali ste heslo, ale je ho potrebné ešte prelomiť. Z Whois aplikácie, prezretím zdrojového kódu projektu, alebo vďaka nejakej nápovede by ste mali vedieť, že na šifrovanie bol použitý bcrypt v javascripte. Je teda potrebné overiť množinu možných hesiel voči tomuto hashu. Skúsite ich preto overiť použitím služby tutorial aplikácie vysvetľujúcej základy bcryptu. Postup je nasledovný:

1. Zapnite BurpSuite a znova sa prepneme do kolónky proxy.
2. Vypnite interceptor a zapnite prehliadač, ktorý má BurpSuite.
3. Prejdite na adresu [http://localhost:5001/](http://localhost:5001/bcryptIntro).
4. V ľavom hornom rohu kliknite na položku v menu s názvom “Bcrypt tutorial”.



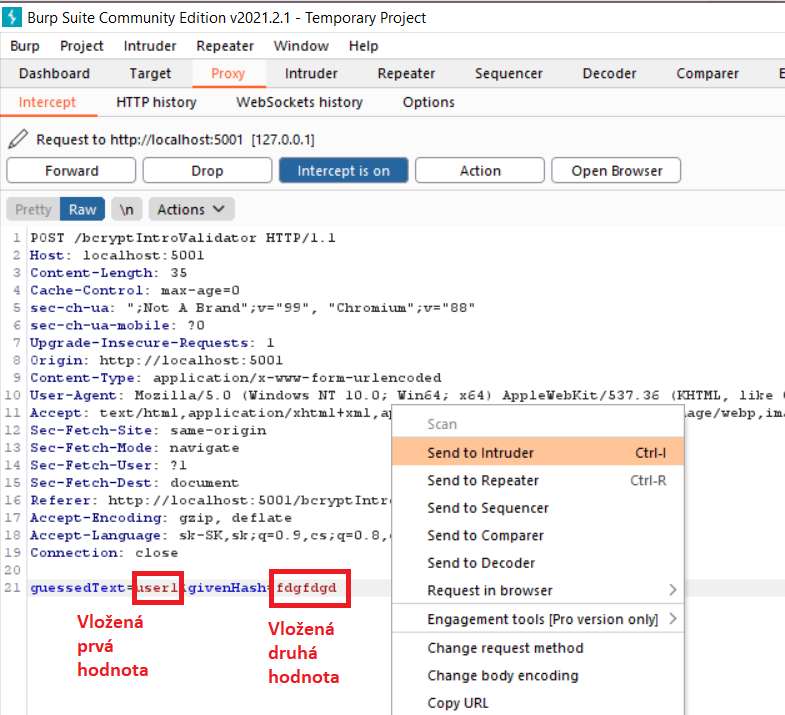
Obrázok 12: Vyhľadanie stránky s tutoriálom pre Bcrypt

1. Preskrolujte na službu s názvom BCrypt validator.



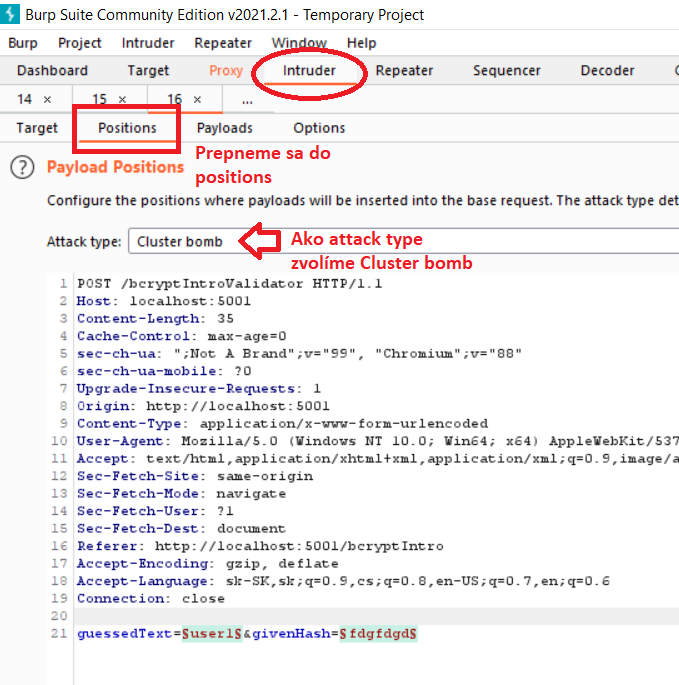
Obrázok 13: Vyvolanie služby pre zistenie či hash vznikol šifrovaním odhadovaného textu

1. Vložte nejaký text do polí Guesed text a Given hash.
2. Zapnite interceptor v BurpSuite.
3. Opäť kliknite ľavým tlačidlom doprostred a v menu vyberte položku “Send to intruder”. V okne ste si mohli všimnúť odosielané hodnoty.



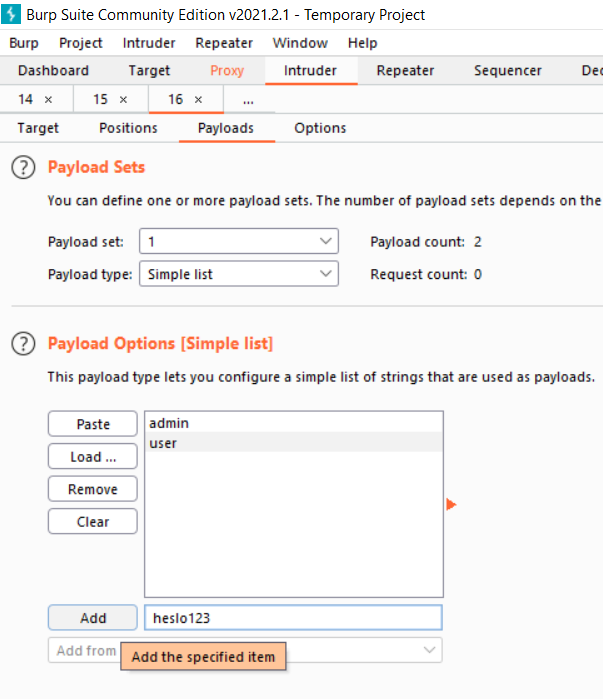
Obrázok 14: Zachytená odoslaná žiadosť na server a odoslanie do intrudera

1. V karte Intruder sa prepnite do podmenu Positions.
2. Následne prenastavte Attack type na Cluster bomb.

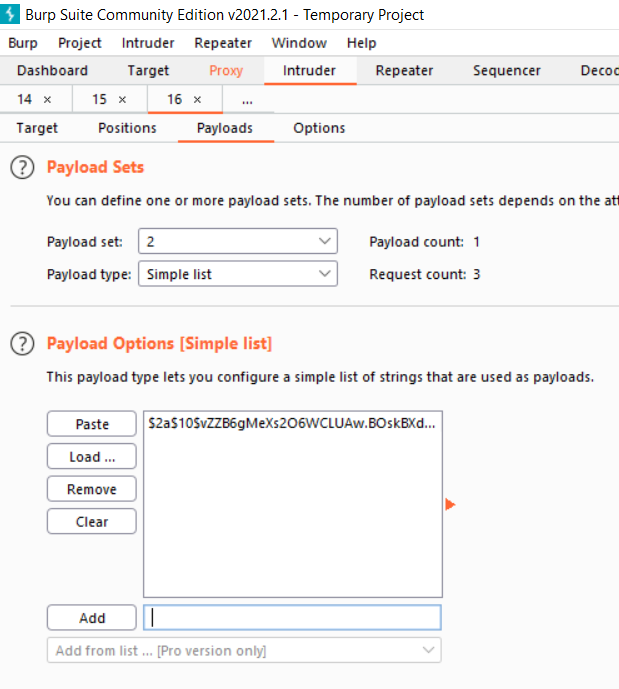


Obrázok 15: Nastavenie typu útoku na Cluster bomb

1. Následne sa prepnite do podmenu karty Intruder s názvom Payloads.
2. Nechajte opäť v prvej časti nastavený Payloads set na 1 a Payload type na “Simple list”. Môžte si všimnúť, že Payloads set je možné prenastaviť na 2. To je preto, že prvé je pre prvý parameter requestu, odhadovaný text a druhý je pre jednu z jeho šifrovaných podôb.
3. Pridajte nižšie v časti Payload options Vami odhadované heslá, opäť také, ktoré sú často používané. Napríklad najčastejšie také, ktoré sú zhodné aj s menom používateľa. Napríklad admin, user, heslo123 a podobne.
4. Prepnite Payloads set v hornej časti s názvom Payloads set na 2. Teraz nastavuje šifrovanú podobu nejakého textu.
5. Opäť v časti Payload options pridajte skopírovaný šifrovaný text používateľa user, ktorý je asistentom.
6. Kliknite na tlačidlo Start attack v pravom hornom rohu.
7. Zobrazil sa Vám zoznam s výsledkami. Keďže služba vracia hodnotu 500, a to v prípade, že hash nebol vytvorený šifrovaním zadaného odhadovaného textu, stačí pozrieť hodnotu výsledného statusu.

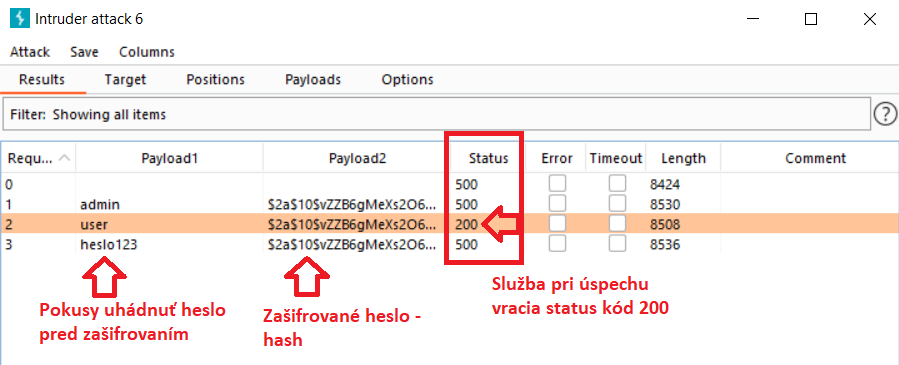


Obrázok 16: Zadanie potencionálnych odhadovaných hesiel – nešifrovaných



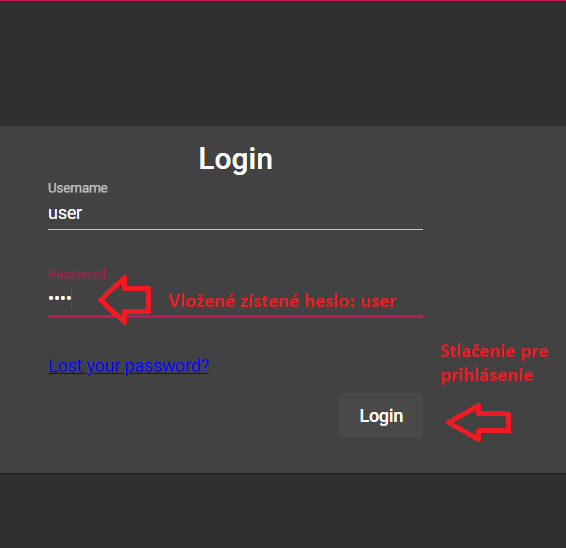
Obrázok 17: Pridanie šifrovanej podoby hesla pre druhý parameter

1. V tabuľke nájdite riadok/riadky s hodnotou status kódu 200. Pozrite sa na Payload číslo 1. Vidíte aké je heslo, ktoré po zašifrovaní môže nadobúdať hash v stĺpci Payload číslo 2. Skopírujte si heslo zo stĺpca Payload číslo 1.

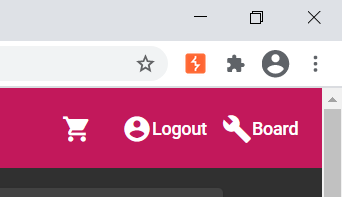


Obrázok 18: Získanie hesla pred zašifrovaním

1. Následne heslo spolu s používateľským menom overte prihlásením sa. Môžte si overiť, že používateľ má naozaj práva asistenta podľa položky Board v hornom menu.



Obrázok 19: Overenie získaného hesla pre používateľa user prihlásením

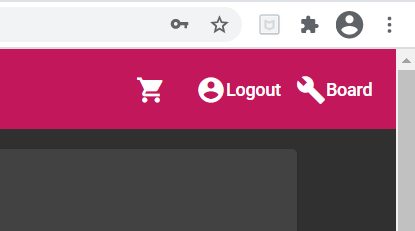


Obrázok 20: Overenie role asistenta

# Použitie SQL injekcie

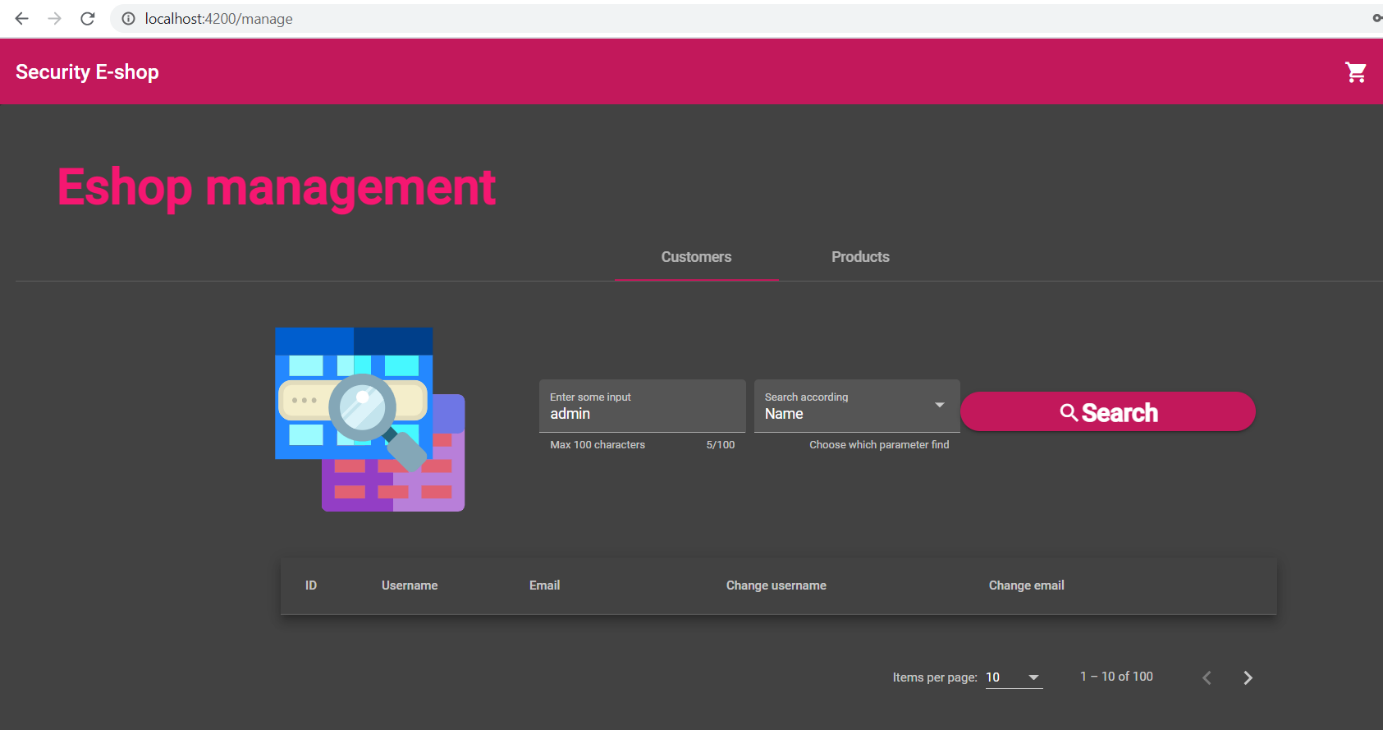
Útočník pri prelamovaní hesiel sa bol schopný dostať do role pracovníka v obchode. Následne má prístup k používateľským emailom a menám. Jeho úlohou bude ale vyhľadať admina, ktorý sa nezobrazuje. Použije SQL injekciu. V tejto časti ponúkame postup pri scenári aplikovania SQL injekcie.

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



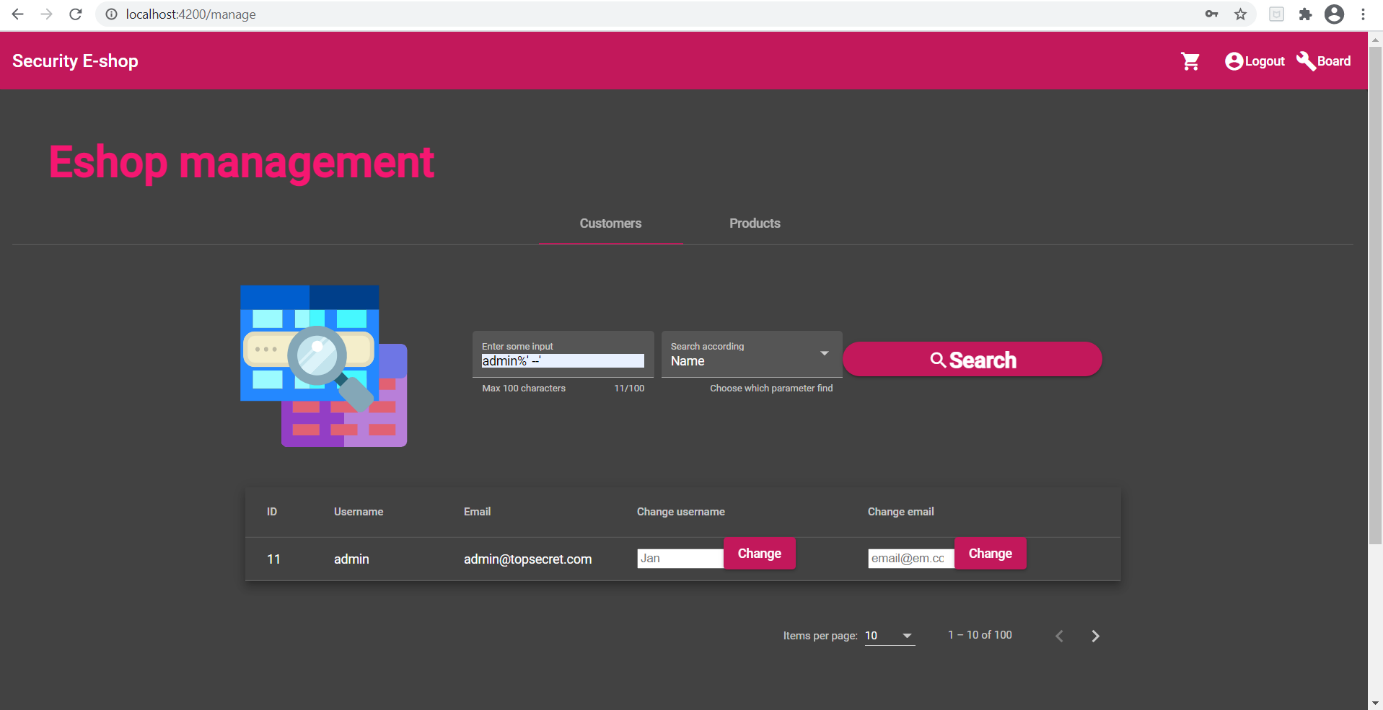
Obrázok 21: Pracovník v obchode má prístup k tabuli používateľov

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



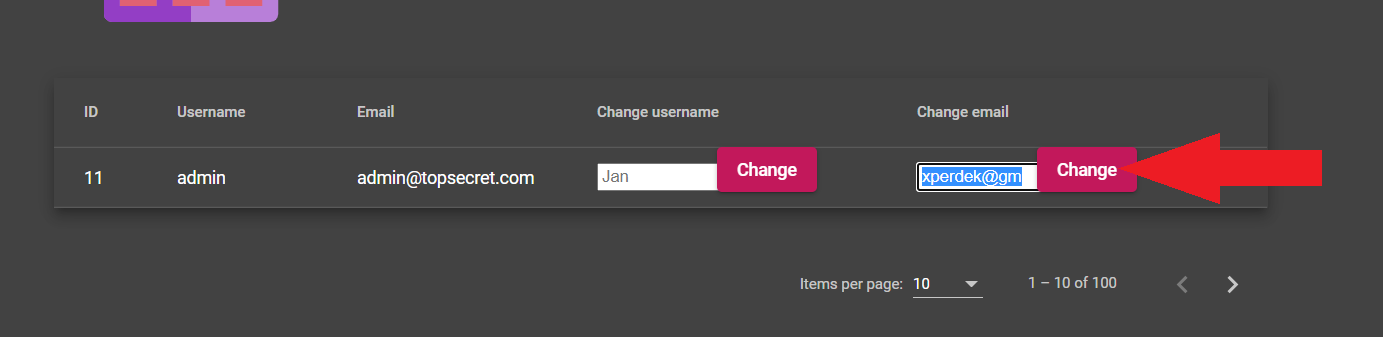
Obrázok 22: Pokus vyhľadať používateľa s menom admin

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



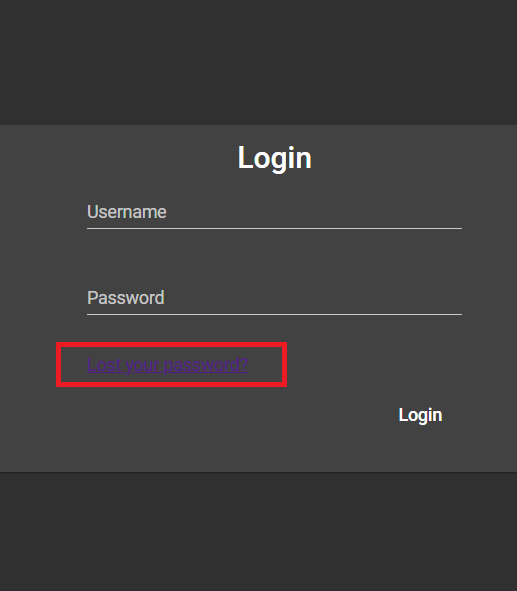
Obrázok 23: Použitie SQL Injekcie pre vyhľadanie používateľa s menom admin

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



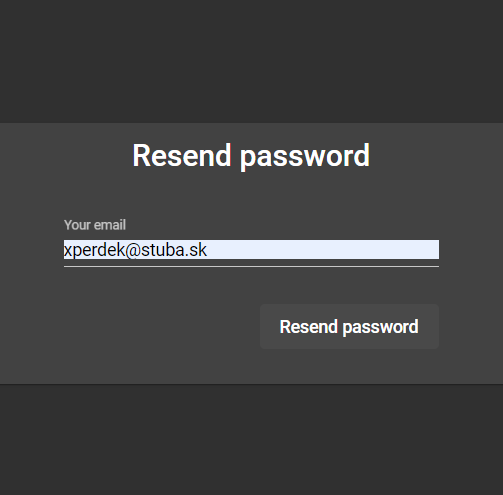
Obrázok 24: Zmena emailovej adresy používateľa admin na svoj vlastný

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



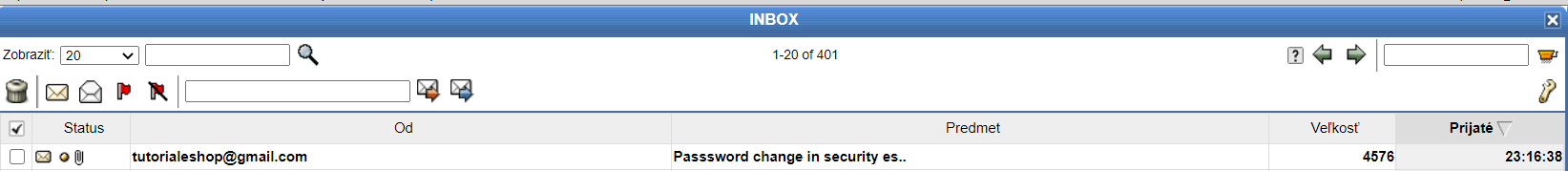
Obrázok 25: Prihlasovací formulár s odkazom na obnovu zabudnutého hesla

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

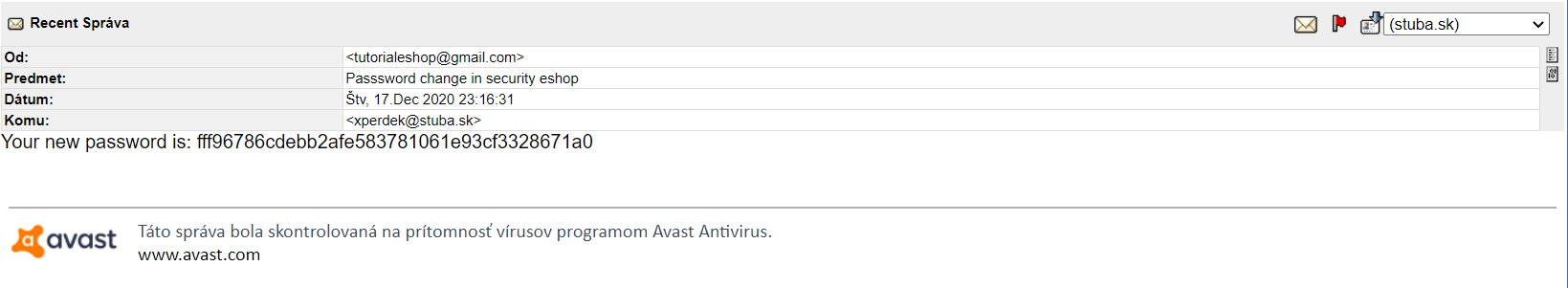


Obrázok 26: Formulár pre pregenerovanie nového hesla

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

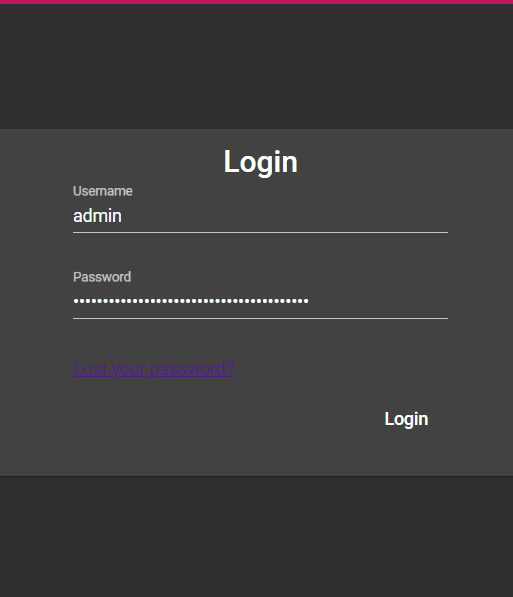


Obrázok 27: Doručenie správy so zmeneným heslom



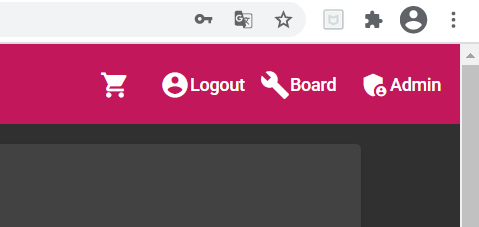
Obrázok 28: Zmenené heslo sa nachádza v správe

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

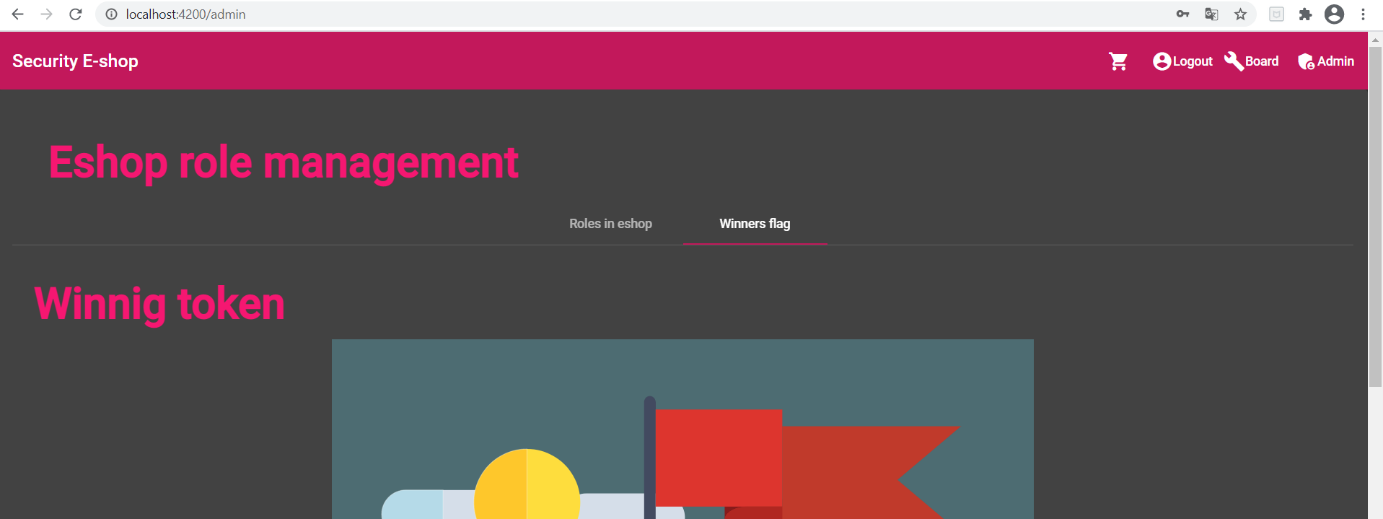


Obrázok 29: Vloženie zmenených údajov do formulára pre prihlásenie

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 30: Používateľ s privilégiom admin má vlastný ovládací panel

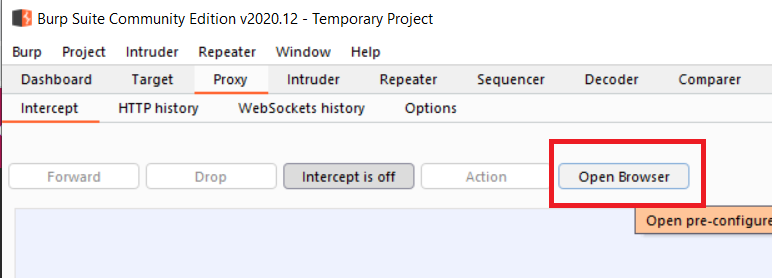


Obrázok 31: Prekliknutie sa na víťazný token

# Ukradnutie produktu z eshopu

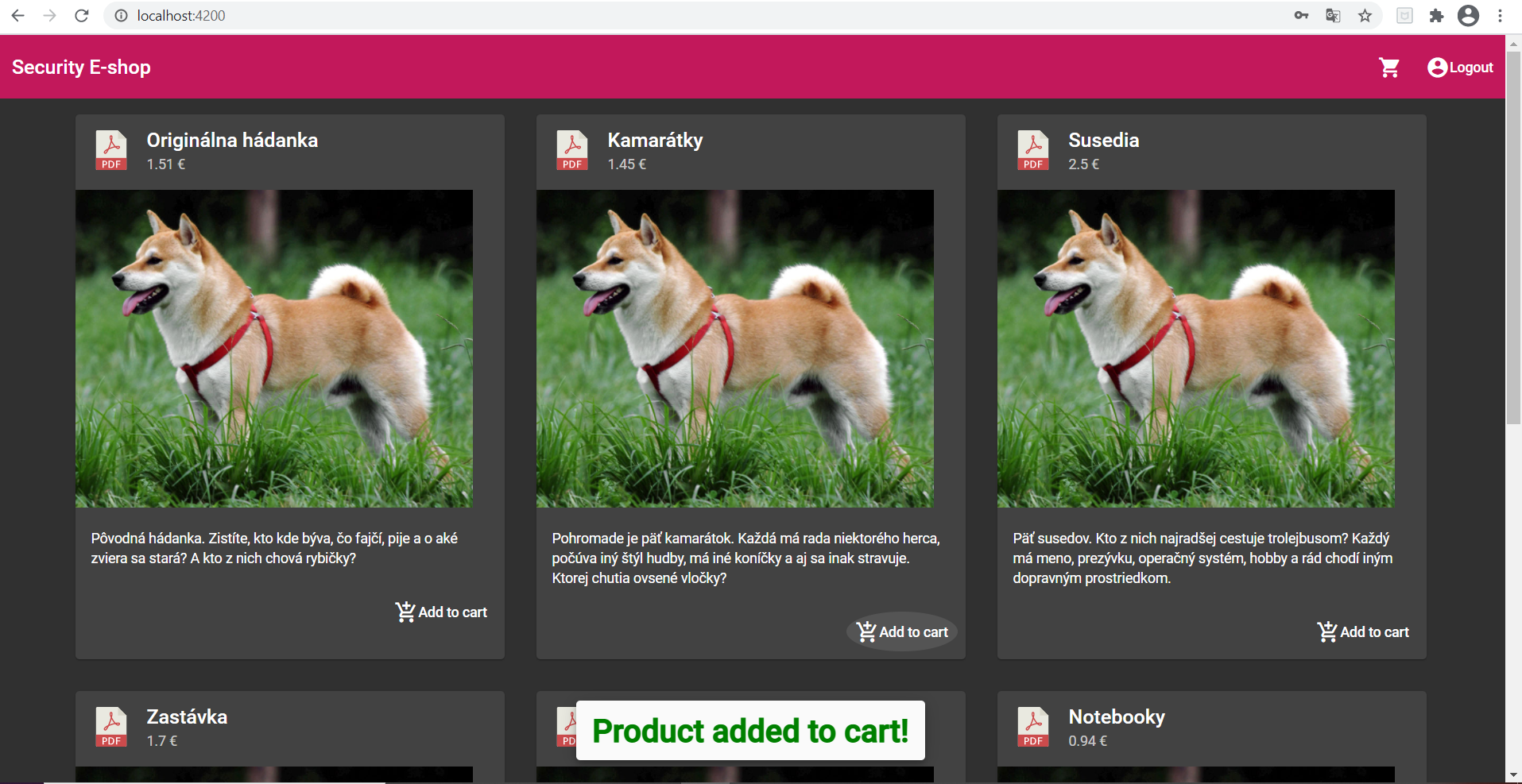
Útočník ukradne produkty z eshopu tým, že pošle vo formulári nulovú hodnotu. Najprv ale musí vytvoriť objednávku.

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



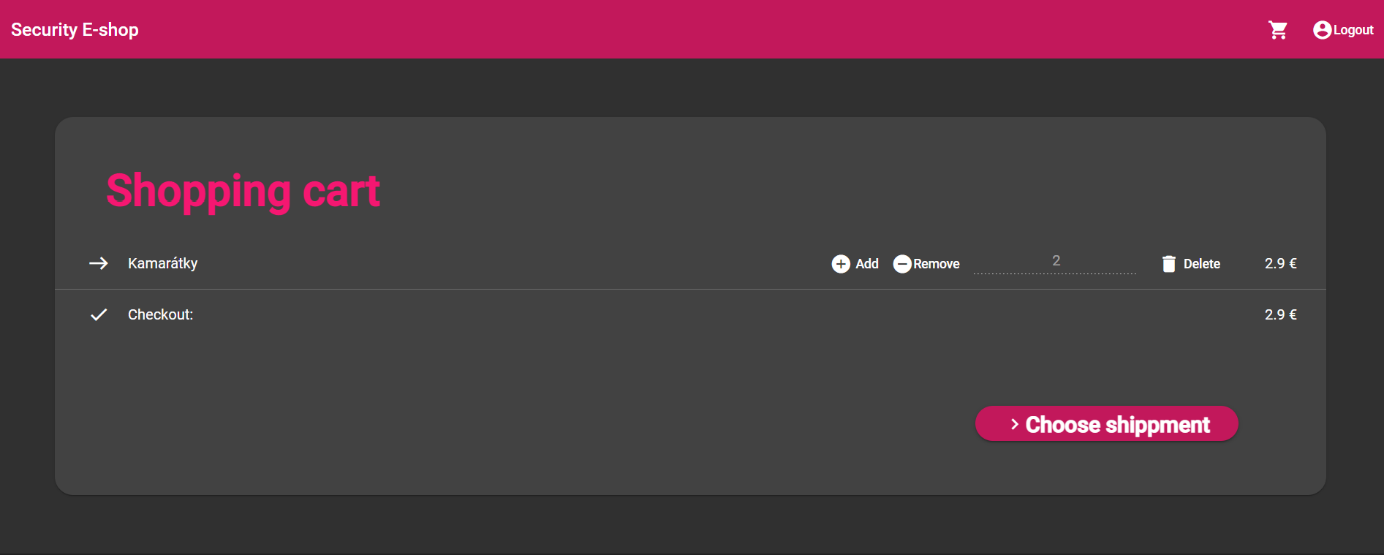
Obrázok 32: Zapnutie burpsuite a otvorenie vlastného prehliadača

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



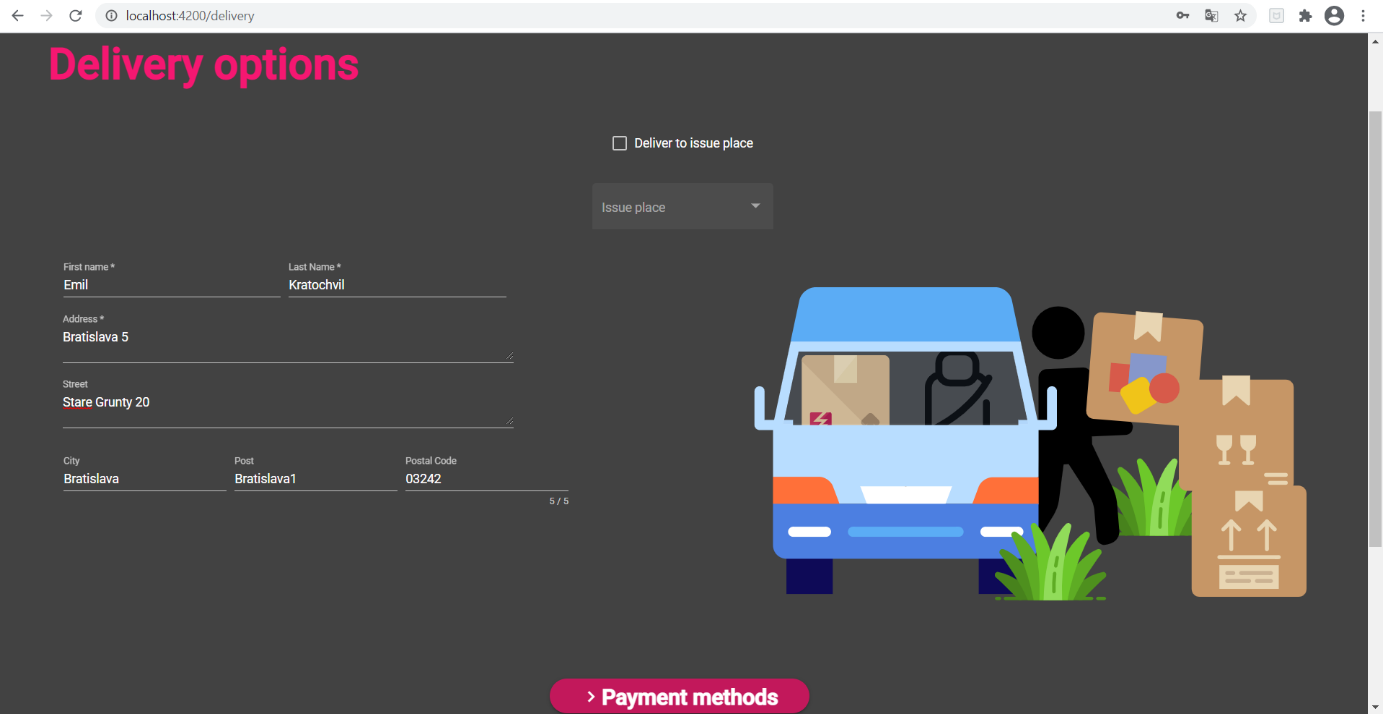
Obrázok 33: Pridanie produktu do košíka

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



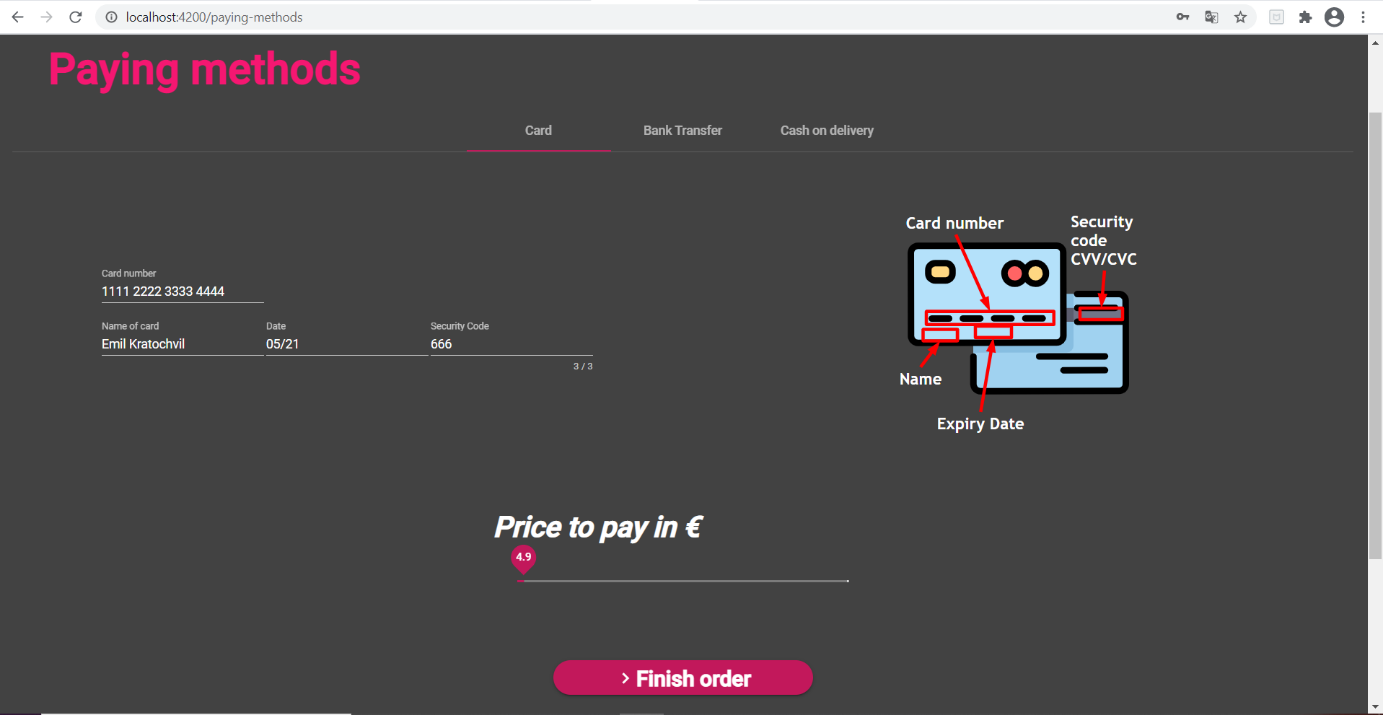
Obrázok 34: Potvrdenie produktov v košíku

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



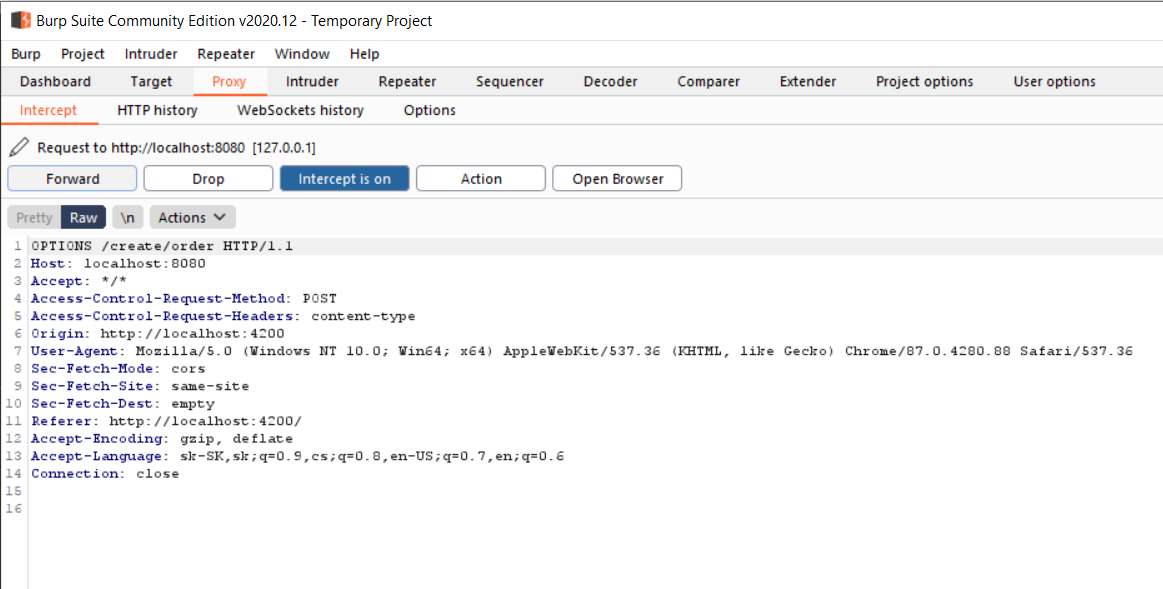
Obrázok 35: Určenie dodacej adresy

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



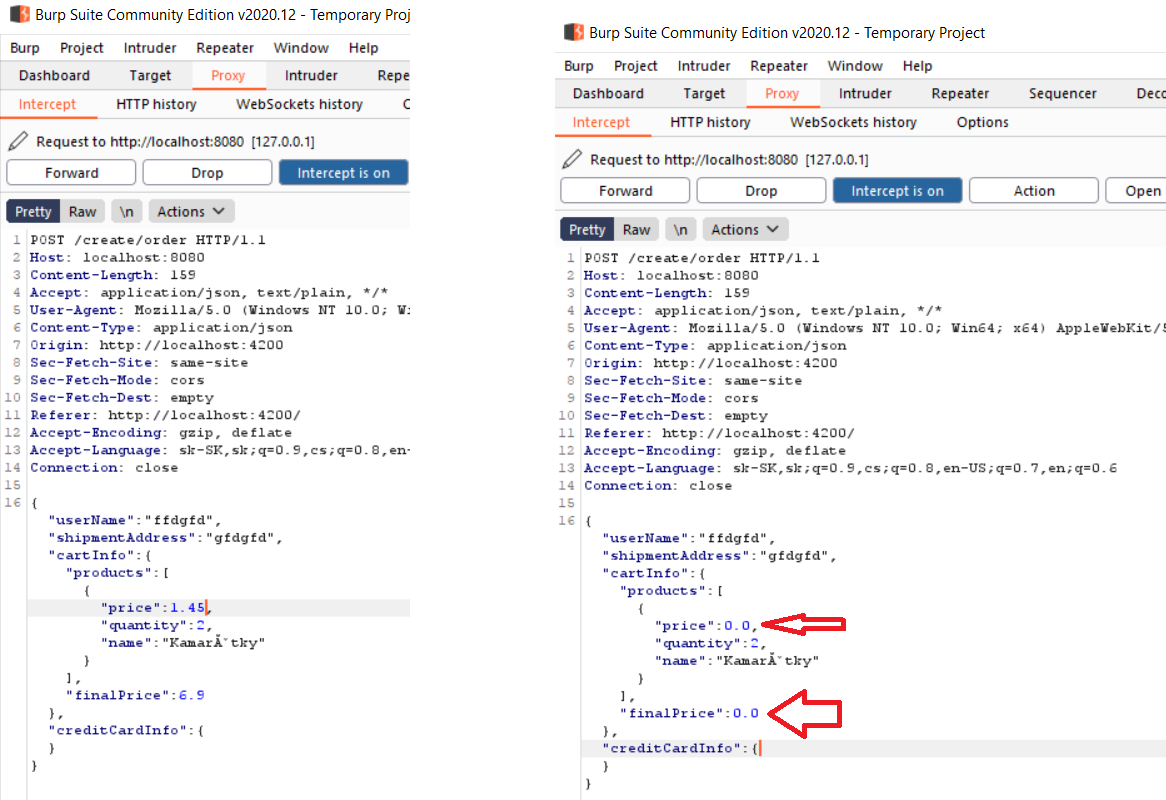
Obrázok 36: Zadanie informácií o platbe a potvrdenie

1. Prvý request prepošlite stlačením tlačidla forward.



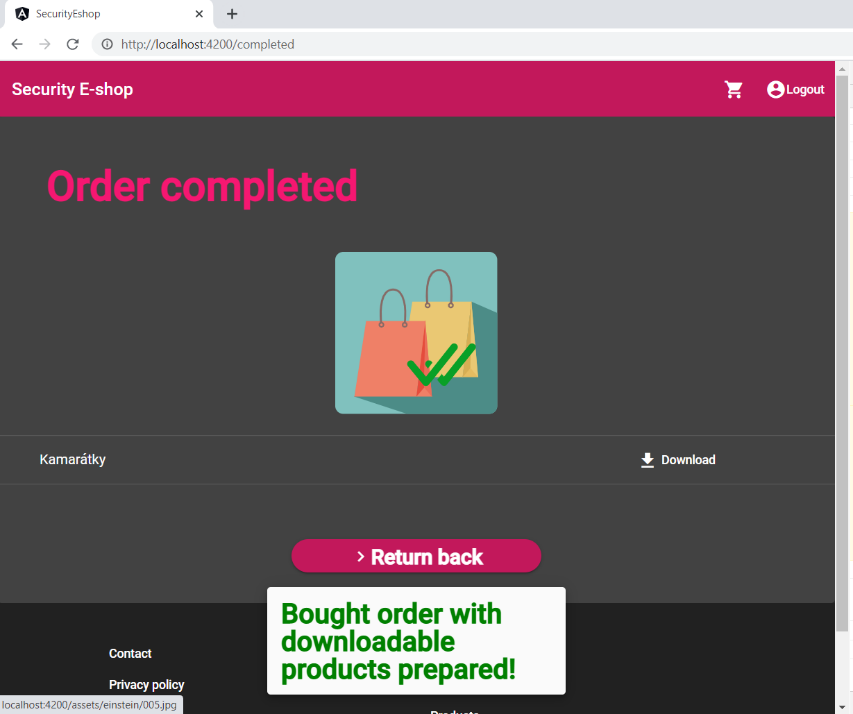
Obrázok 37: Ignorovanie prvého requestu

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



Obrázok 38: Zmena informácií v druhom requeste

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

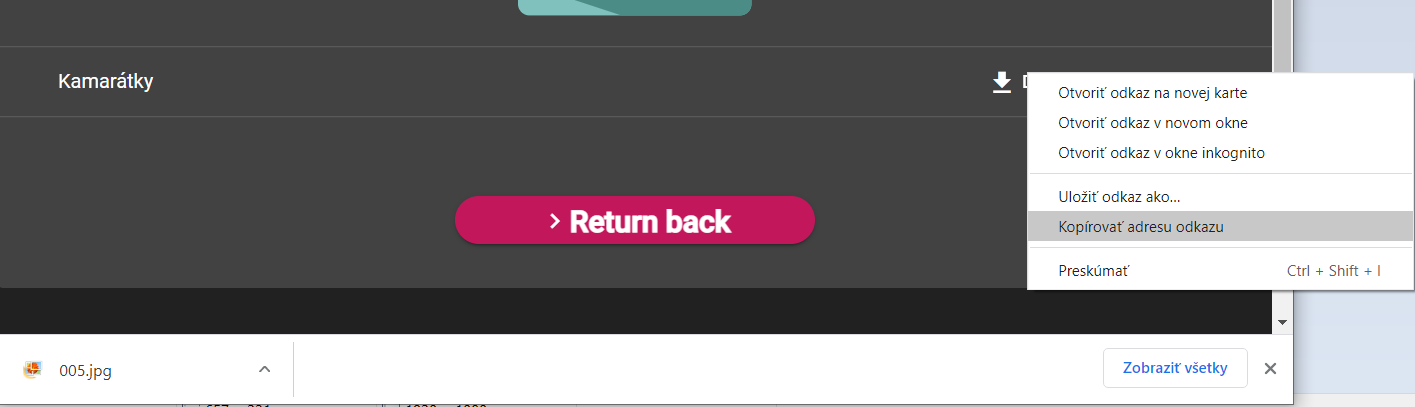


Obrázok 39: Stiahnutie ukradnutých produktov

# Získanie prístupu k súborom

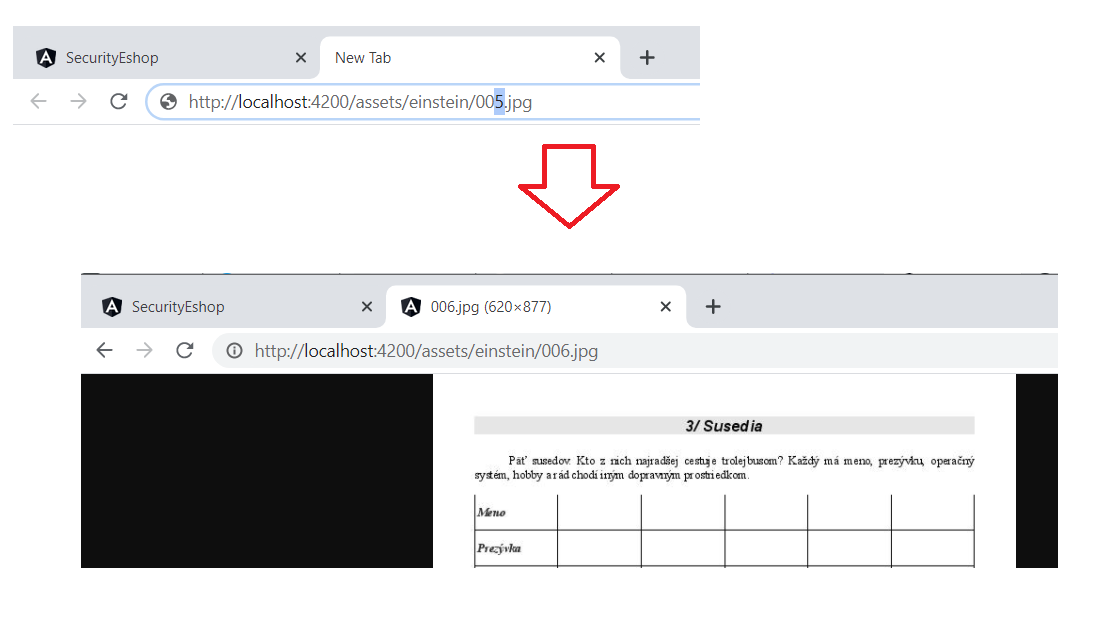
Útočník by mal vedieť, že ako technológia bol použitý Angulár. Na základe tejto informácie by mal byť schopný dostať sa k verejne uloženým súborom na stránke zadaním do prehliadača cestu k assets/images. Už je len potrebné zistiť presnú cestu. Pri minulom scenári s ukradnutím produktu si ale môže všimnúť, 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 40: Získanie odkazu na stiahnutý obsah

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



Obrázok 41: Vyskúšanie podobnej adresy s inkrementovaným číslom obrázka