

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

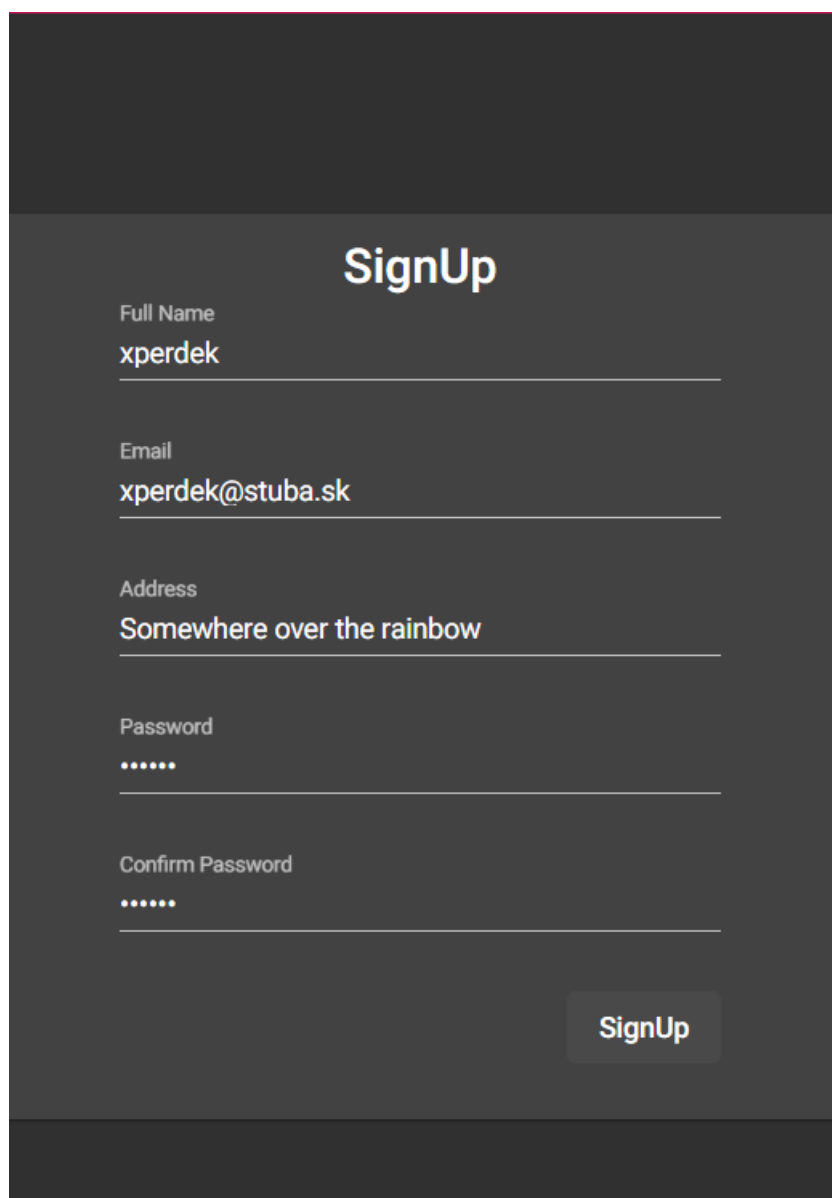
**Vypracoval:** Jakub Perdek

**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.

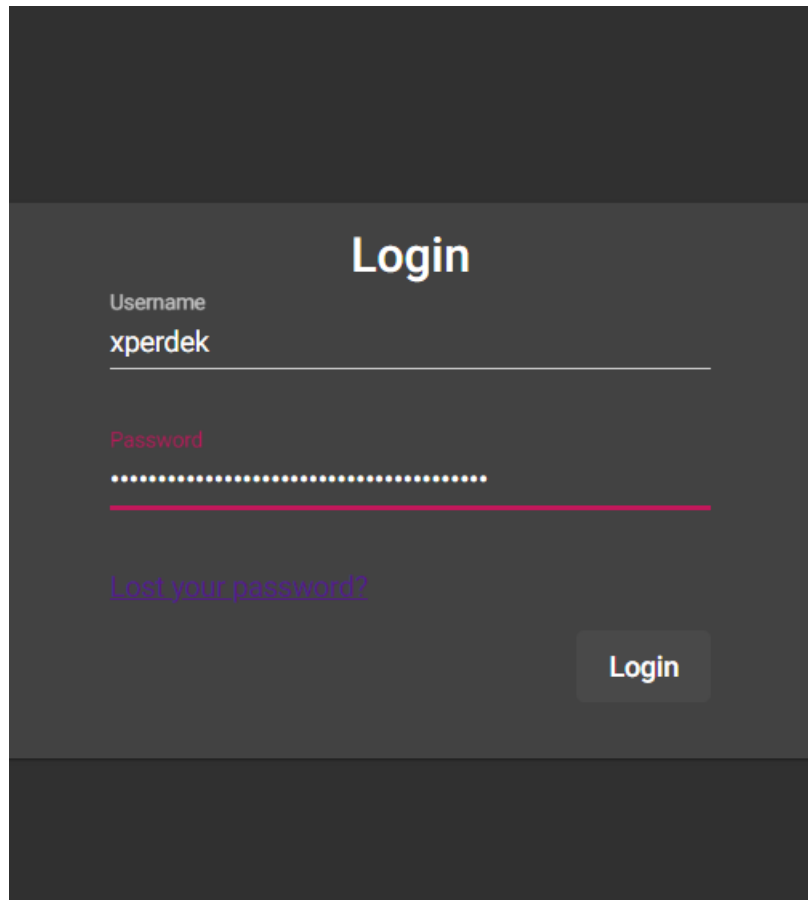
1. Zaregistrujte sa stlačením na tlačidlo SignUp v hornom rohu stránky.



The image shows a dark-themed user registration form. At the top, the title "SignUp" is displayed in a large, bold, white font. Below the title, there are five input fields, each with a label and a value: "Full Name" with "xperdek", "Email" with "xperdek@stuba.sk", "Address" with "Somewhere over the rainbow", "Password" with ".....", and "Confirm Password" with ".....". Each input field has a thin white underline. 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 word "Login" in a dark gray font.

Username  
xperdek

Password  
.....

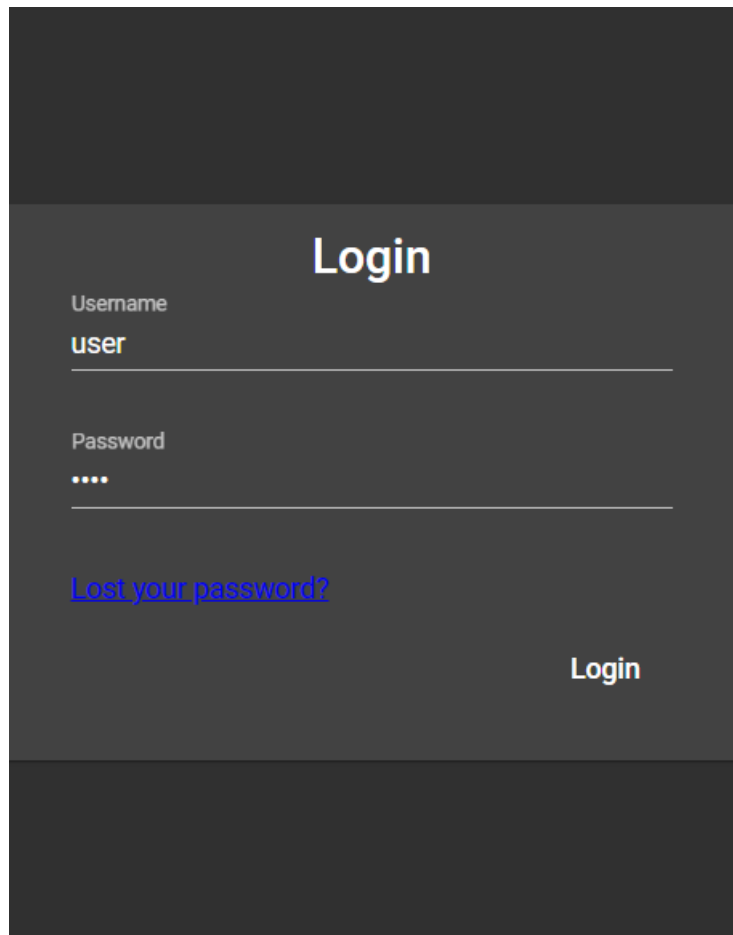
[Lost your password?](#)

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.



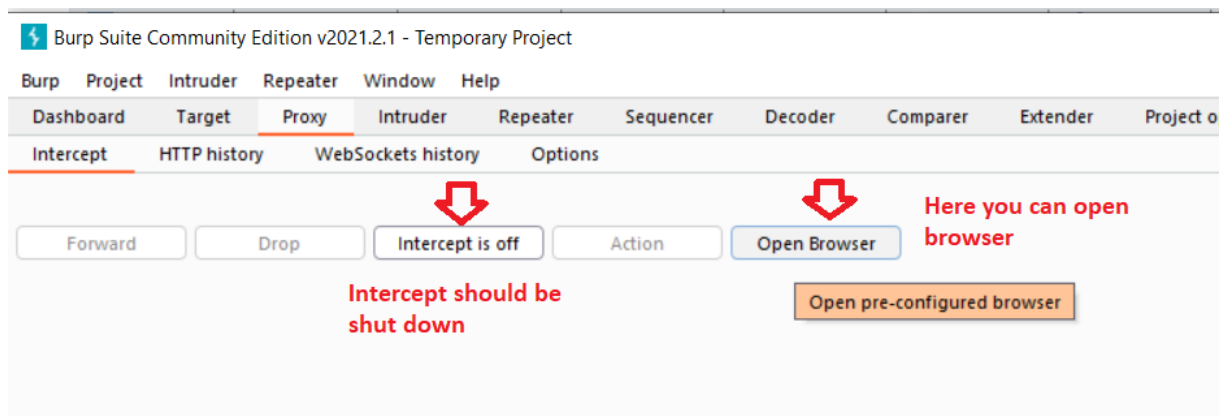
The image shows a dark-themed login interface. At the top, the word "Login" is displayed in a large, white, sans-serif font. Below it, there are two input fields. The first is labeled "Username" in a small, light gray font, and the text "user" is entered in white. The second is labeled "Password" in 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 area, there is a white "Login" button.

Obrázok 3: Aplikovanie jednoduchého hesla user

# Prelamovanie hesiel slovníkovým útokom

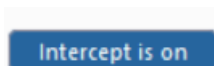
Útočník môže zrealizovať slovníkový útok na základe získaných informácií z login stránky. K užitočným informáciám sa dostanete na základe nasledujúceho postupu:

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



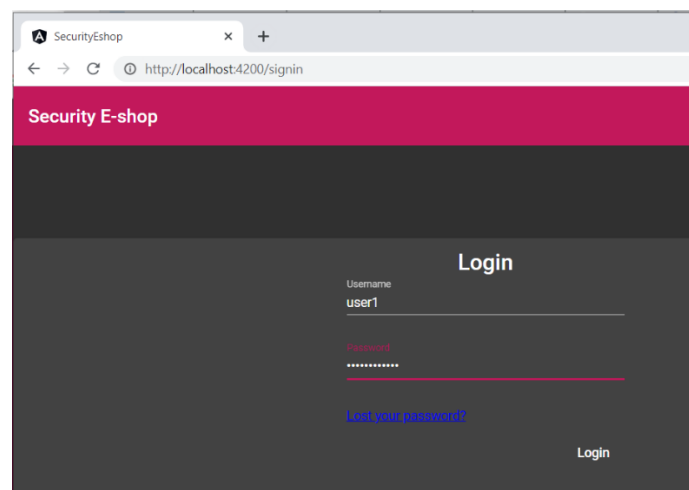
Obrázok 4: Otvorenie prehliadača a interceptor v BurpSuite

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



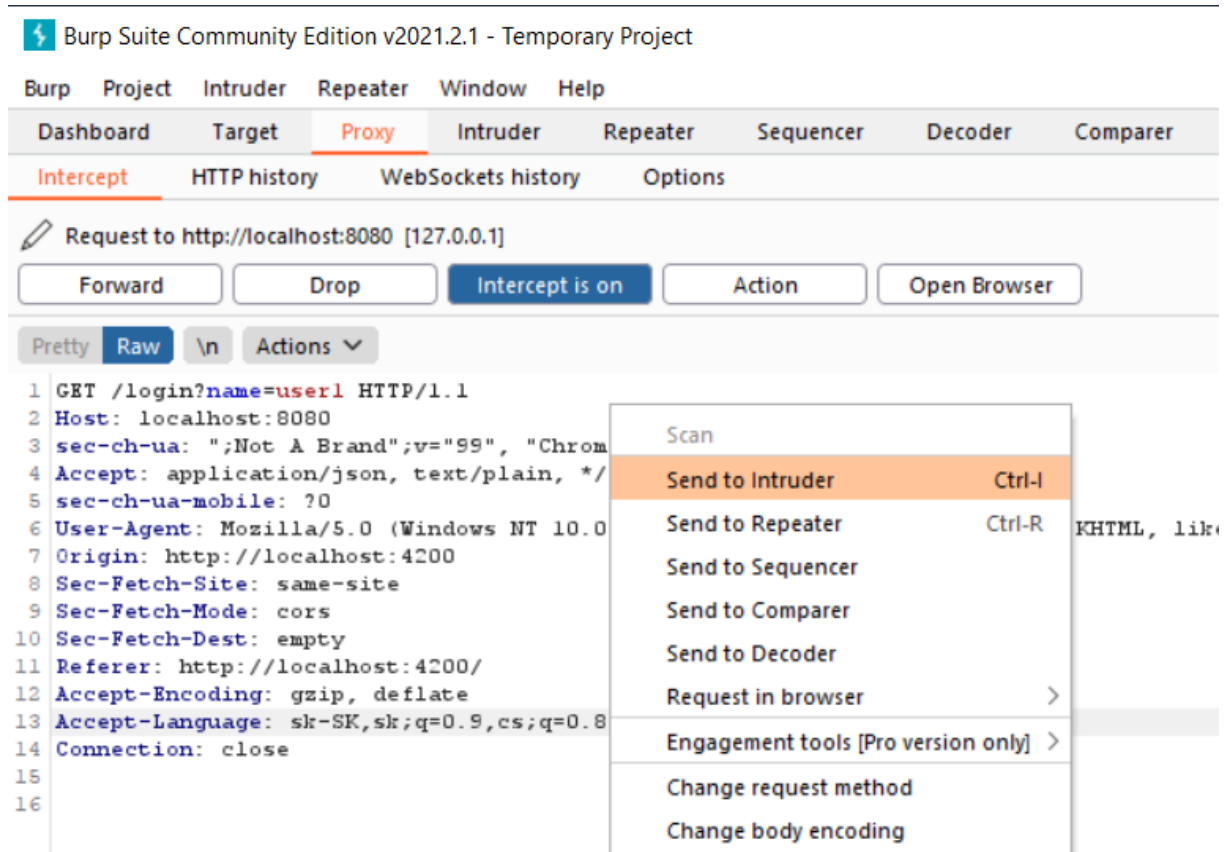
Obrázok 5: Zapnutie interceptora

6. Pokúste sa prihlásiť s ľubovoľným menom a heslom.



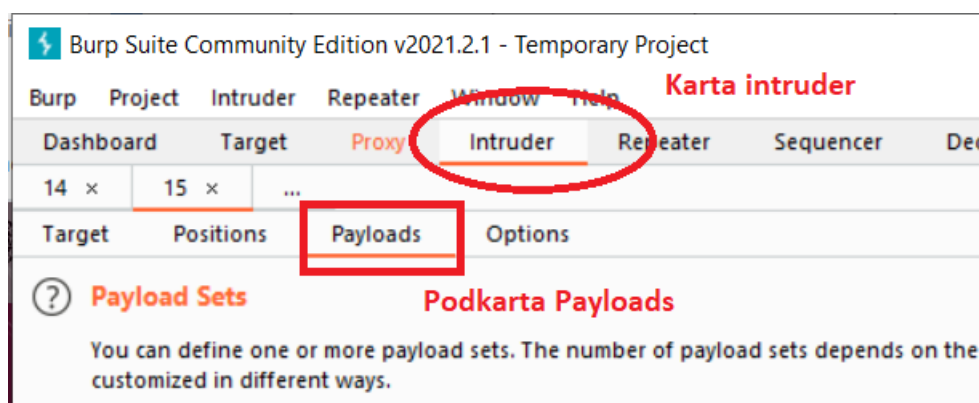
Obrázok 6: Pokus o prihlásenie v stavanom prehliadači BurpSuitu

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



Obrázok 7: Odoslanie requestu do intrudera

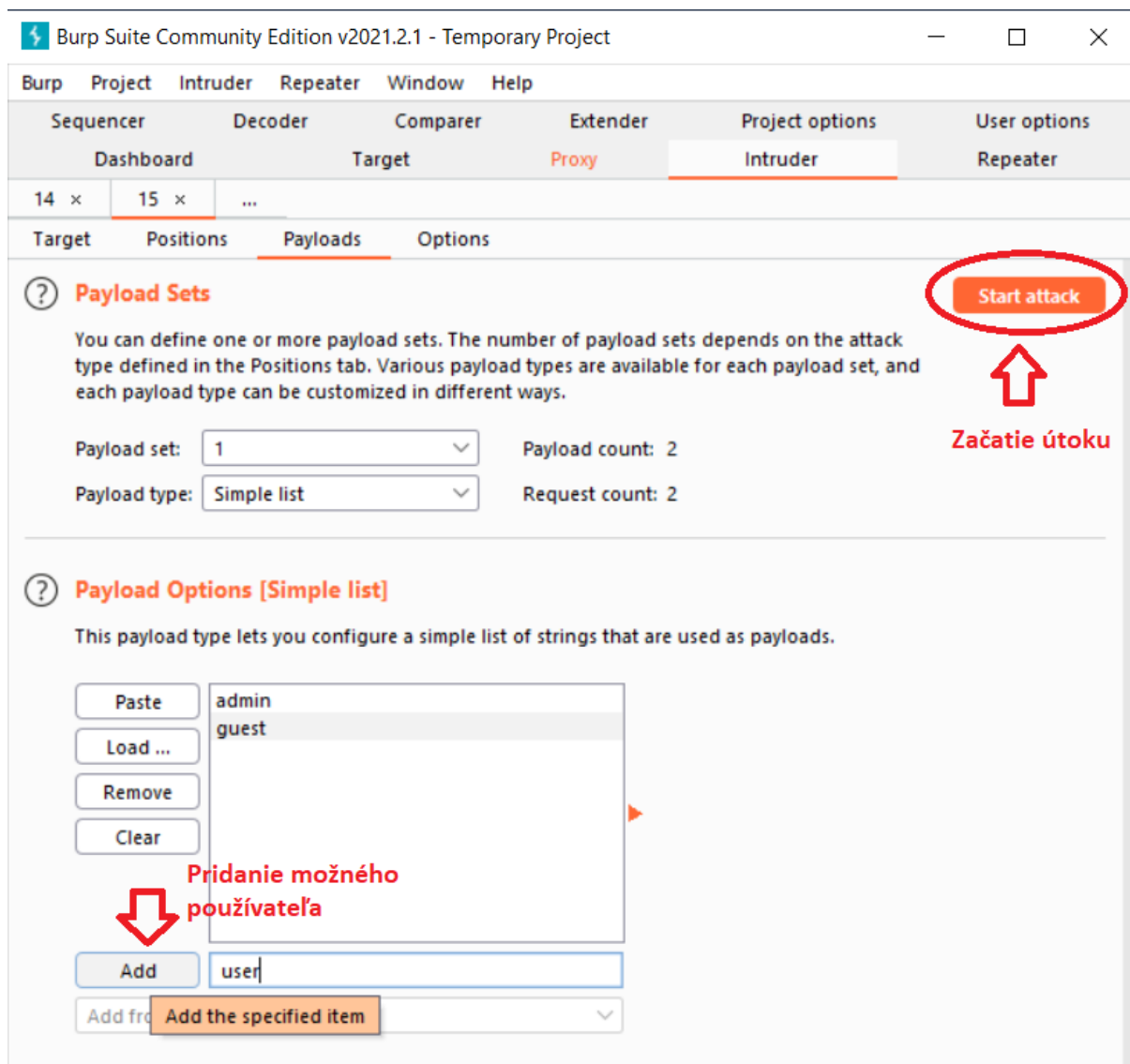
10. Následne kliknite na otvorenú položku Intruder-a.
11. Rozkliknite podmenu Payloads v položke Intruder-a.



12. Obrázok 8: Presunutie sa na položku Payloads v Intruderovi

13. Vo vrchnej časti Payload Sets rozkliknutej karty v BurpSuite nechajte nastavené Payload set na 1 a Payload type na Simple list.

14. 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.
15. Zvoľte položku “Start attack”.



Obrázok 9: Zadanie zoznamu potencionálnych používateľov a začatie útoku

16. Otvorí sa okno, v ktorom podľa vráteného statusu môžete zistiť, ktorí používatelia existujú v systéme.
17. Kliknite na jeden z riadkov, ktorý má status 200.
18. Prepnite sa na kartu Response, v okne ktoré sa zobrazí nižšie.
19. Môžete zistiť, že aplikácia dostala heslo spolu s emailom 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.

Intruder attack 5

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Requ...	Payload	Status	Error	Timeout	Length	Comment
0		500	<input type="checkbox"/>	<input type="checkbox"/>	5591	
1	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	350	
2	guest	500	<input type="checkbox"/>	<input type="checkbox"/>	5591	
3	user	200	<input type="checkbox"/>	<input type="checkbox"/>	392	

admin a user existujú v systéme

Obrázok 10: Zistenie existujúcich používateľov v systéme

20. Skopírujte heslo usera, ktorý je asistent.

Intruder attack 5

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Requ...	Payload	Status	Error	Timeout	Length	Comment
0		500	<input type="checkbox"/>	<input type="checkbox"/>	5591	
1	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	350	
2	guest	500	<input type="checkbox"/>	<input type="checkbox"/>	5591	
3	user	200	<input type="checkbox"/>	<input type="checkbox"/>	392	

Request Response

Pretty Raw Render \n Actions

```

1 HTTP/1.1 200
2 Vary: Origin
3 Vary: Access-Control-Request-Method
4 Vary: Access-Control-Request-Headers
5 Access-Control-Allow-Origin: *
6 Content-Type: application/json
7 Date: Fri, 12 Mar 2021 21:13:07 GMT
8 Connection: close
9 Content-Length: 145
10
11 {
  "id": 5,
  "name": "user",
  "email": "user@user.sk",
  "password": "$2a$10$vZZB6gMeXs206WCLUAw.B0skBXdlqPa0F.1e7fzYxlrsofswQCc0Sa",
  "priviledges": "assistant"
}

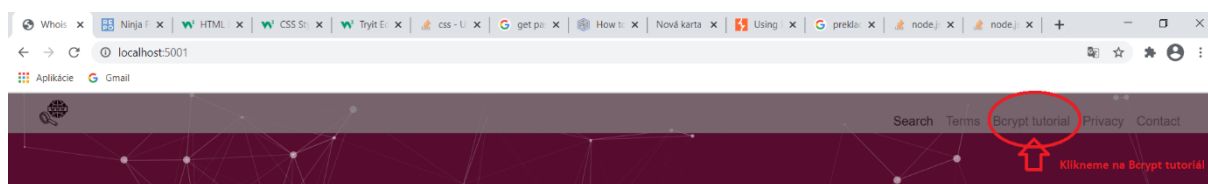
```

Obrázok 11: Získanie zašifrovaného hesla asistenta s používateľským menom user



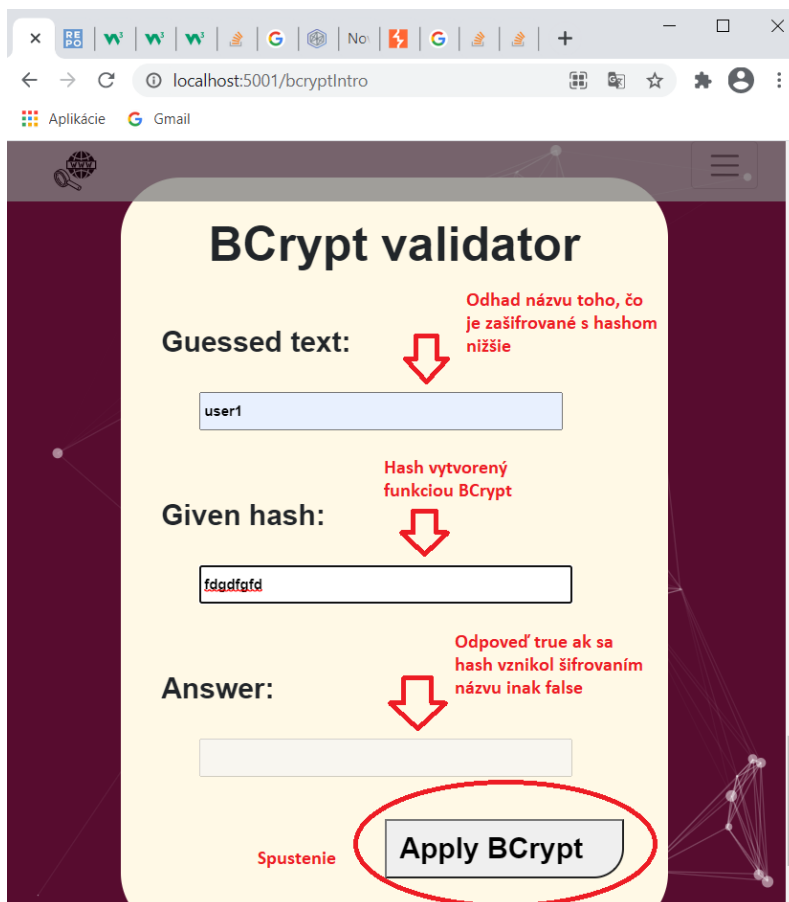
Získali ste heslo, ale je ho potrebné ešte prelomiť. Z Whois aplikácie, prezretím zdrojového kódu projektu, alebo vďaka nejakej nápovede by ste mali vedieť, že na šifrovanie bol použitý bcrypt v javascripte. Je teda potrebné overiť množinu možných hesiel voči tomuto hashu. Skúsate ich preto overiť použitím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

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



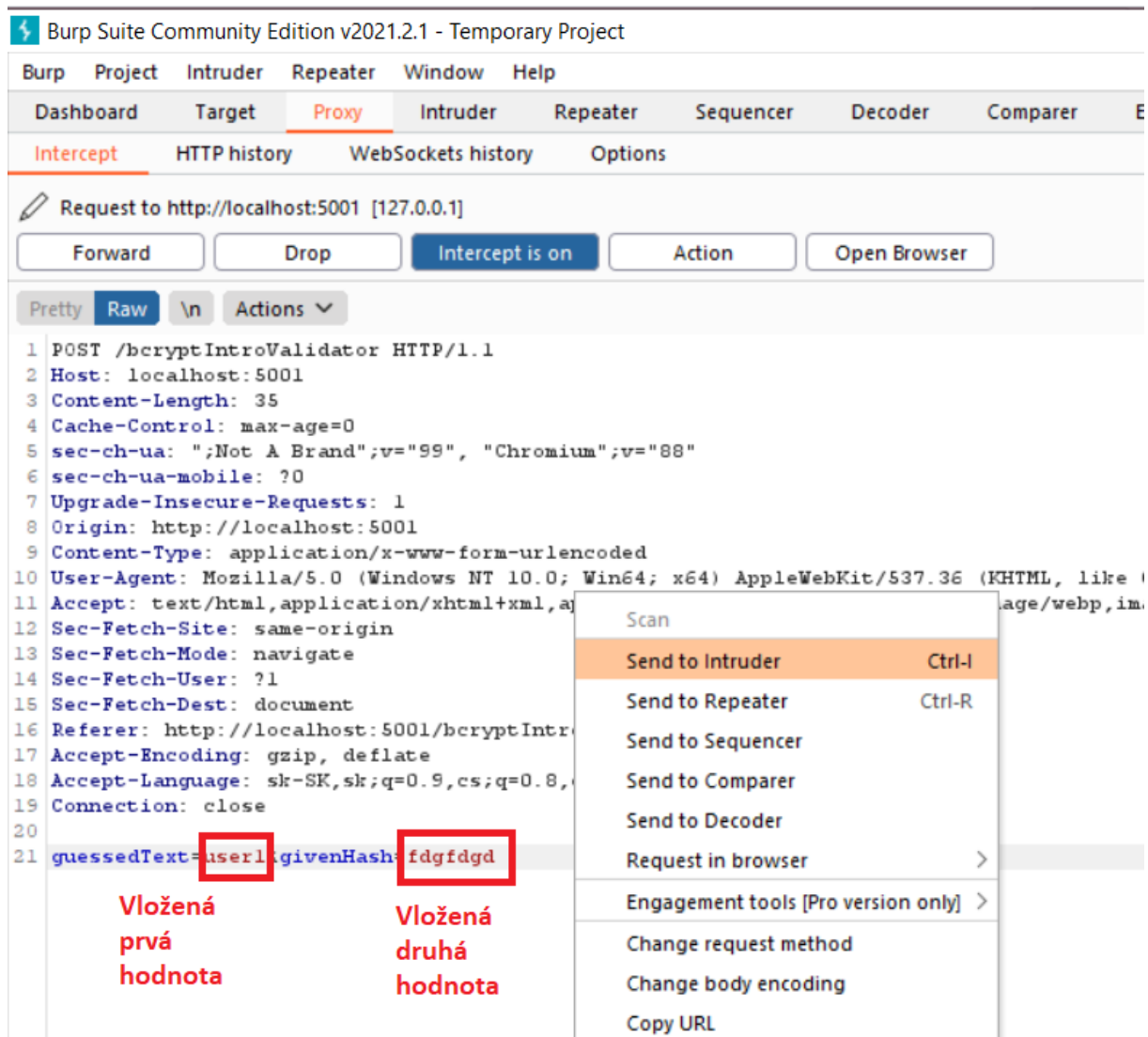
Obrázok 12: Vyhľadanie stránky s tutoriálom pre Bcrypt

5. Preskrolujte na službu s názvom BCrypt validator.



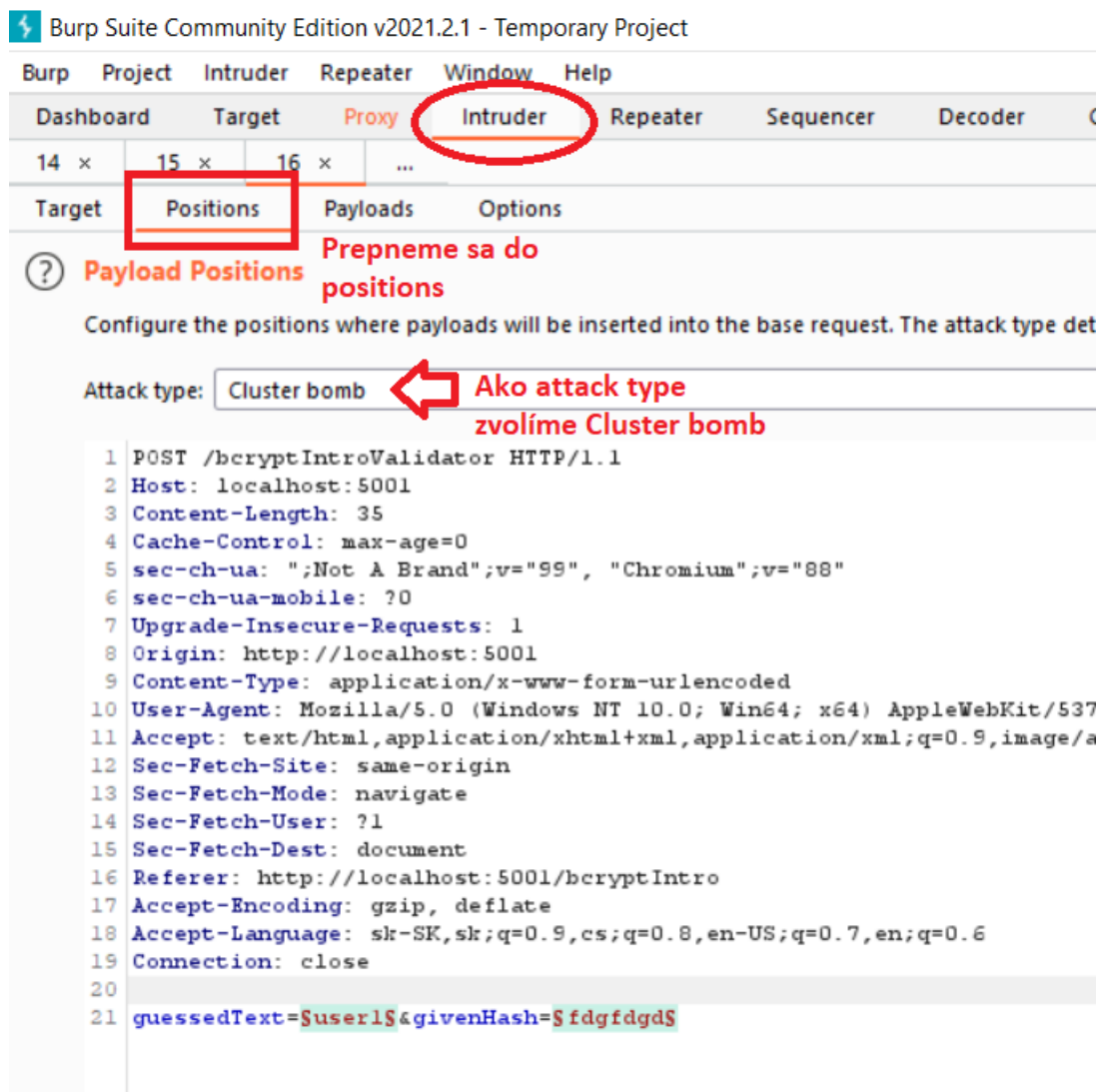
Obrázok 13: Vyvolanie služby pre zistenie či hash vznikol šifrovaním odhadovaného textu

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



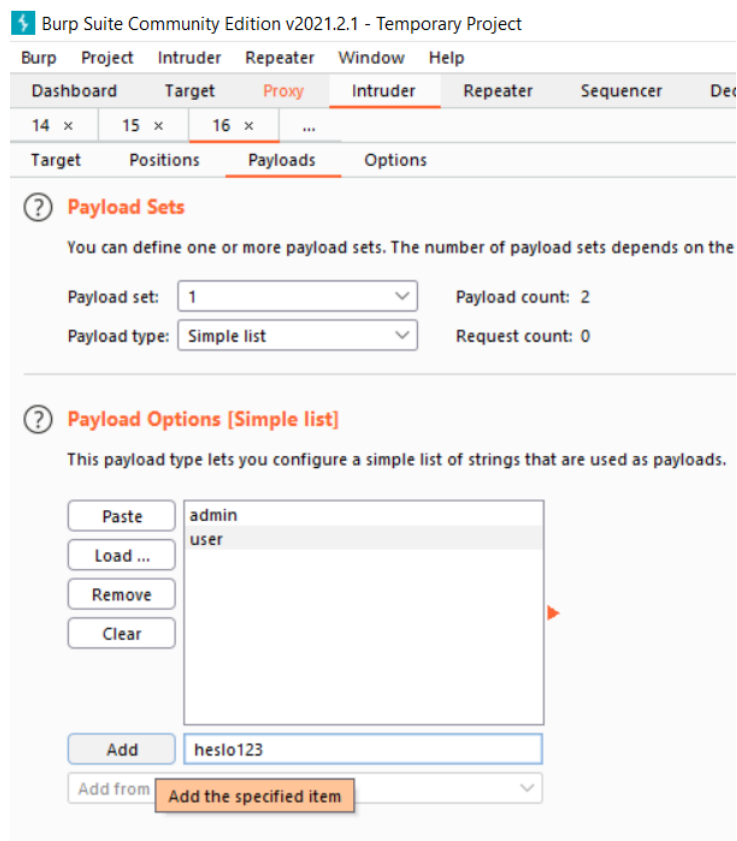
Obrázok 14: Zachytená odoslaná žiadosť na server a odoslanie do intrudera

9. V karte Intruder sa prepnete do podmenu Positions.
10. Následne prenasťte Attack type na Cluster bomb.

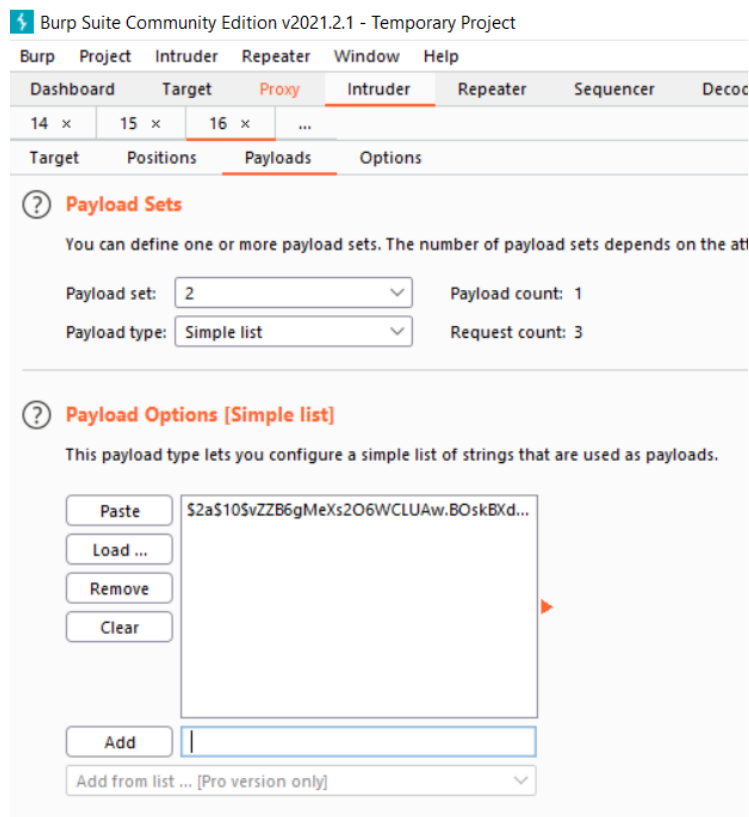


Obrázok 15: Nastavenie typu útoku na Cluster bomb

11. Následne sa prepnete do podmenu karty Intruder s názvom Payloads.
12. Nechajte opäť v prvej časti nastavený Payloads set na 1 a Payload type na "Simple list". Môžete 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.
13. 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.
14. Prepnete Payloads set v hornej časti s názvom Payloads set na 2. Teraz nastavuje šifrovanú podobu nejakého textu.
15. Opäť v časti Payload options pridajte skopírovaný šifrovaný text používateľa user, ktorý je asistentom.
16. Kliknite na tlačidlo Start attack v pravom hornom rohu.
17. 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: Zadané potencionálnych odhadovaných hesiel – nešifrovaných



Obrázok 17: Pridanie šifrovanej podoby hesla pre druhý parameter

18. 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.

Intruder attack 6

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Requ...	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			500	<input type="checkbox"/>	<input type="checkbox"/>	8424	
1	admin	\$2a\$10\$vvZZB6gMeXs2O6...	500	<input type="checkbox"/>	<input type="checkbox"/>	8530	
2	user	\$2a\$10\$vvZZB6gMeXs2O6...	200	<input type="checkbox"/>	<input type="checkbox"/>	8508	
3	heslo123	\$2a\$10\$vvZZB6gMeXs2O6...	500	<input type="checkbox"/>	<input type="checkbox"/>	8536	

↑ Pokusy uhádnuť heslo pred zašifrovaním

↑ Zašifrované heslo - hash

← Služba pri úspechu vracia status kód 200

Obrázok 18: Získanie hesla pred zašifrovaním

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

Login

Username  
user

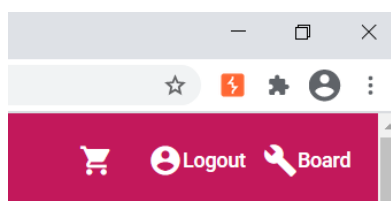
Password  
... Vložené zistené heslo: user

Lost your password?

Login

Stlačenie pre prihlásenie

Obrázok 19: Overenie získaného hesla pre používateľa user prihlásením

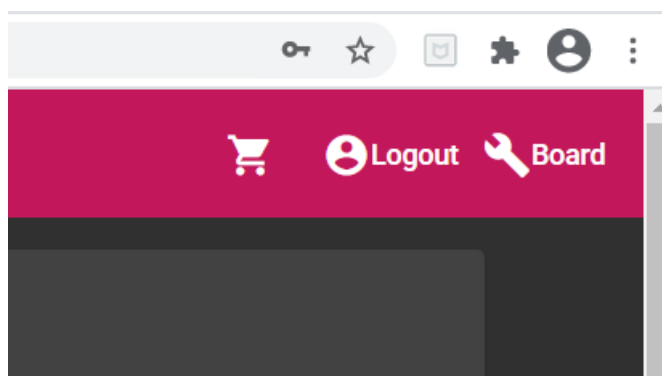


Obrázok 20: Overenie role asistenta

# Použitie SQL injekcie

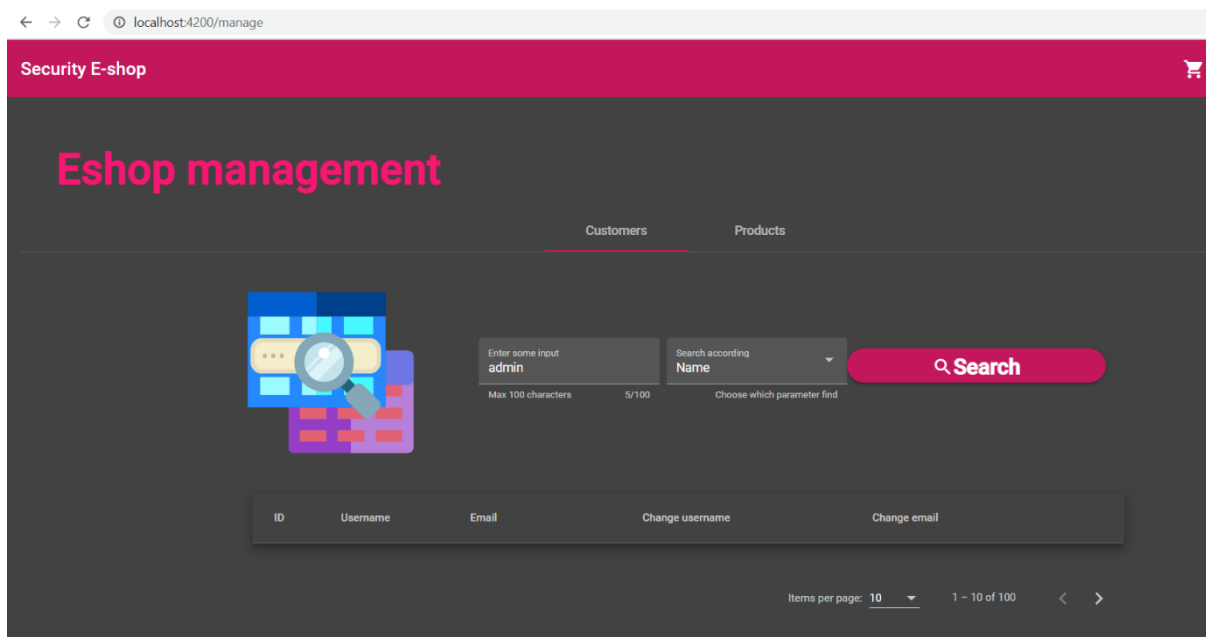
Útočník pri prelamaní hesiel sa bol schopný dostať do role pracovníka v obchode. Následne má prístup k používateľským emailom a menám. Jeho úlohou bude ale vyhľadať admina, ktorý sa nezobrazuje. Použije SQL injekciu. V tejto časti ponúkame postup pri scenári aplikovania SQL injekcie.

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



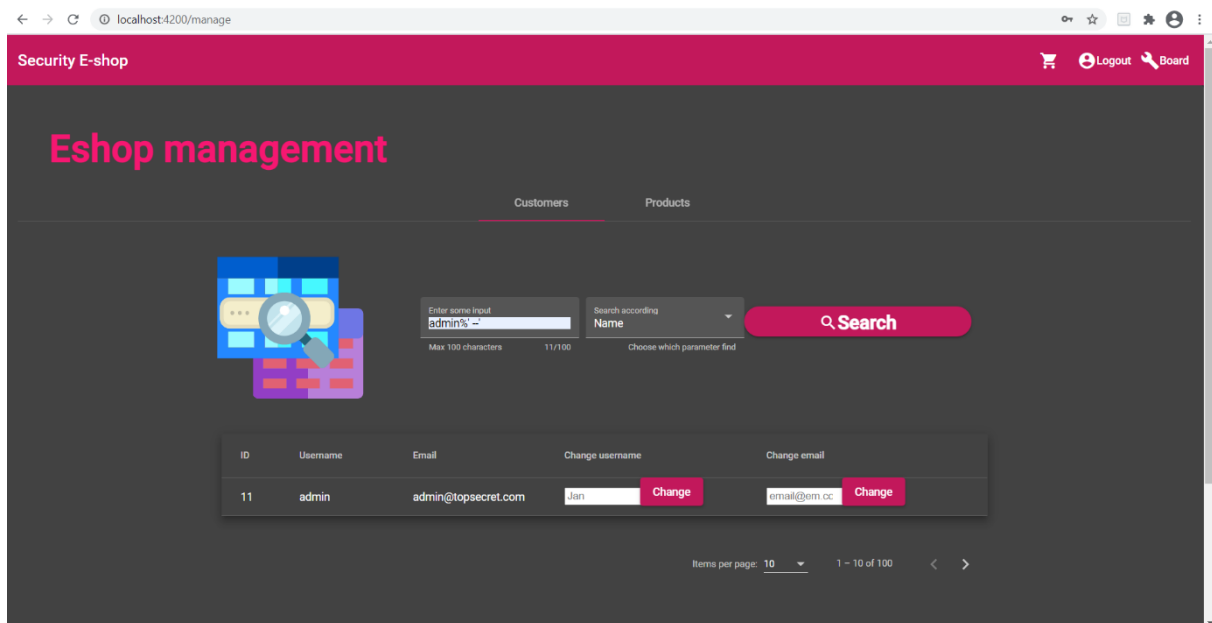
Obrázok 21: Pracovník v obchode má prístup k tabuli používateľov

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



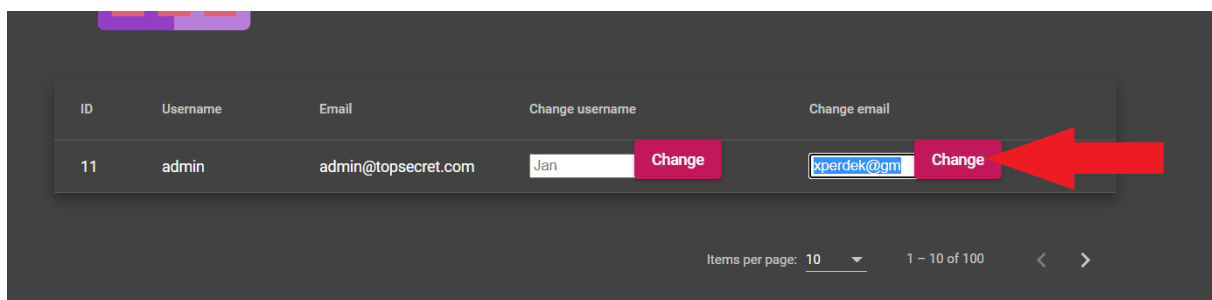
Obrázok 22: Pokus vyhľadať používateľa s menom admin

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



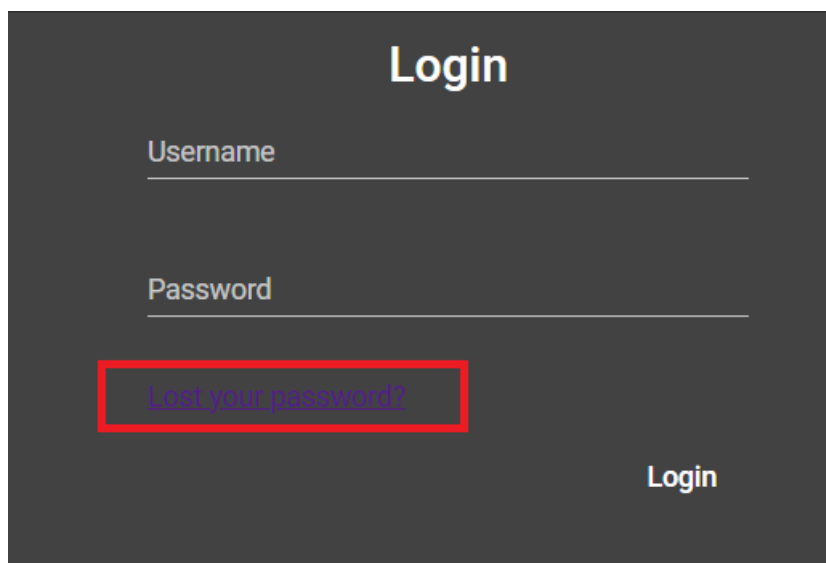
Obrázok 23: Použitie SQL Injekcie pre vyhládanie používateľa s menom admin

4. 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

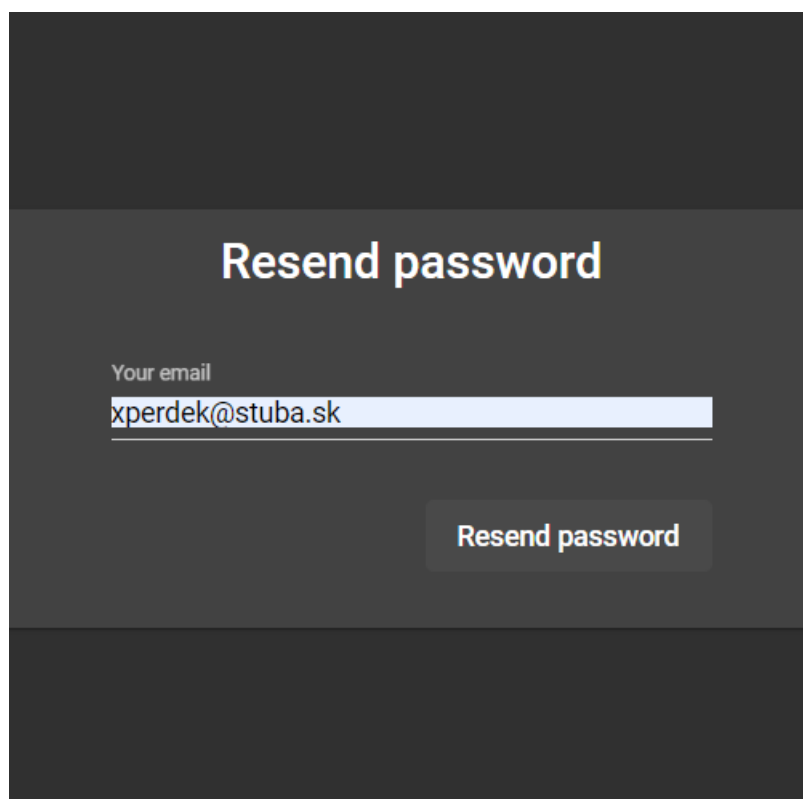
5. Odhláste sa kliknite na tlačidlo pre opätovné prihlásenie. Namiesto prihlásenia ale kliknite na odkaz Lost your password?



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 link, there is a "Login" button with white text on a dark background.

Obrázok 25: Prihlasovací formulár s odkazom na obnovu zabudnutého hesla

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

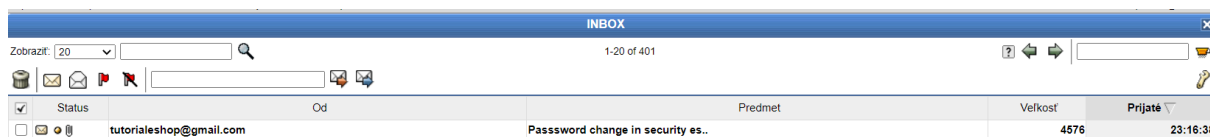


The image shows a dark-themed form for resetting a password. At the top, the text "Resend password" is centered in a large, white, sans-serif font. Below it, there is a label "Your email" in a small, white, sans-serif font. Underneath the label is an input field containing the email address "xperdek@stuba.sk"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

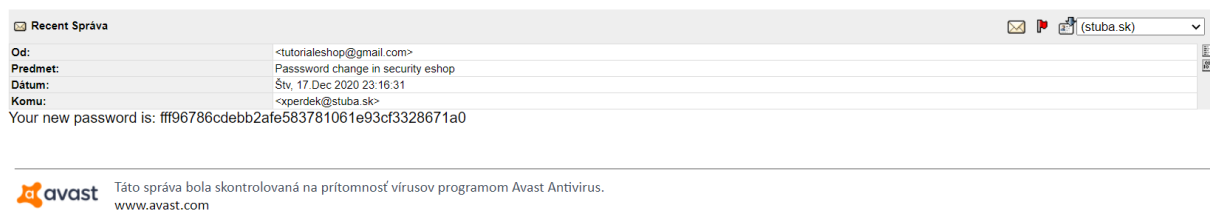
Obrázok 26: Formulár pre pregenerovanie nového hesla



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



Obrázok 27: Doručenie správy so zmeneným heslom



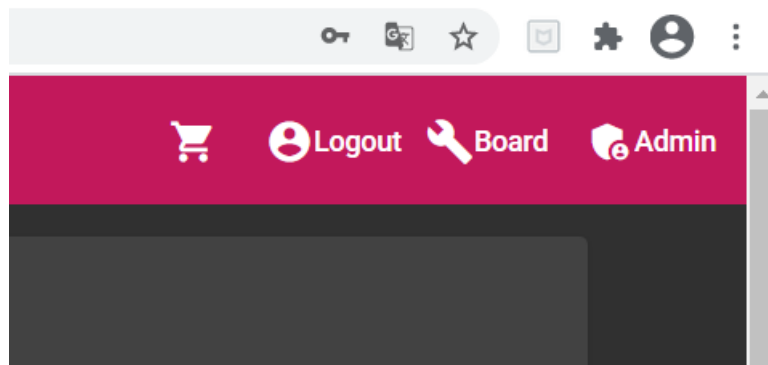
Obrázok 28: Zmenené heslo sa nachádza v správe

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

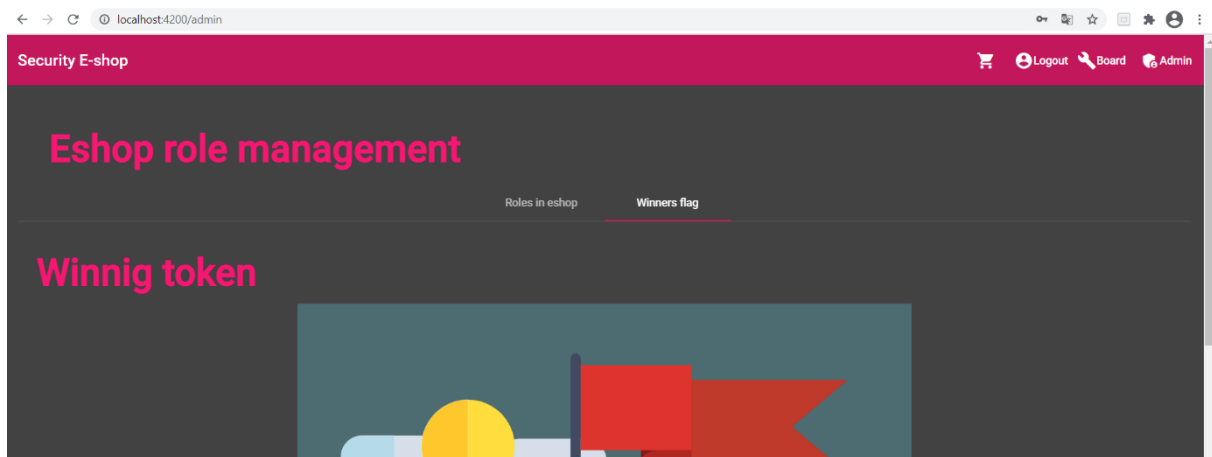
A screenshot of a login page. The background is dark grey. At the top, the word 'Login' is written in large white letters. Below it, there are two input fields: 'Username' with the text 'admin' and 'Password' with a masked password represented by dots. Below the password field, there is a link that says 'Lost your password?'. At the bottom right, there is a 'Login' button.

Obrázok 29: 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 30: Používateľ s privilégiom admin má vlastný ovládací panel

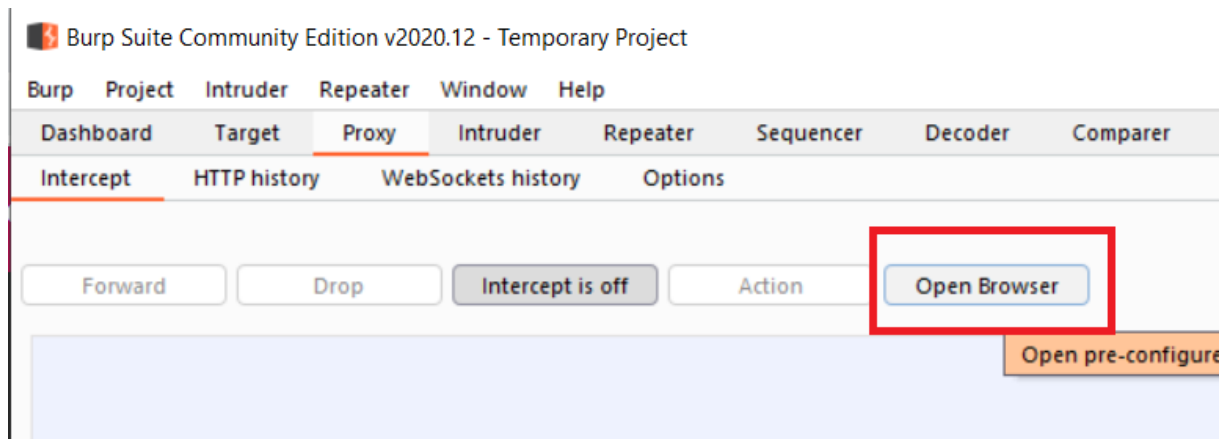


Obrázok 31: Prekliknutie sa na víťazný token

# Ukradnutie produktu z eshopu

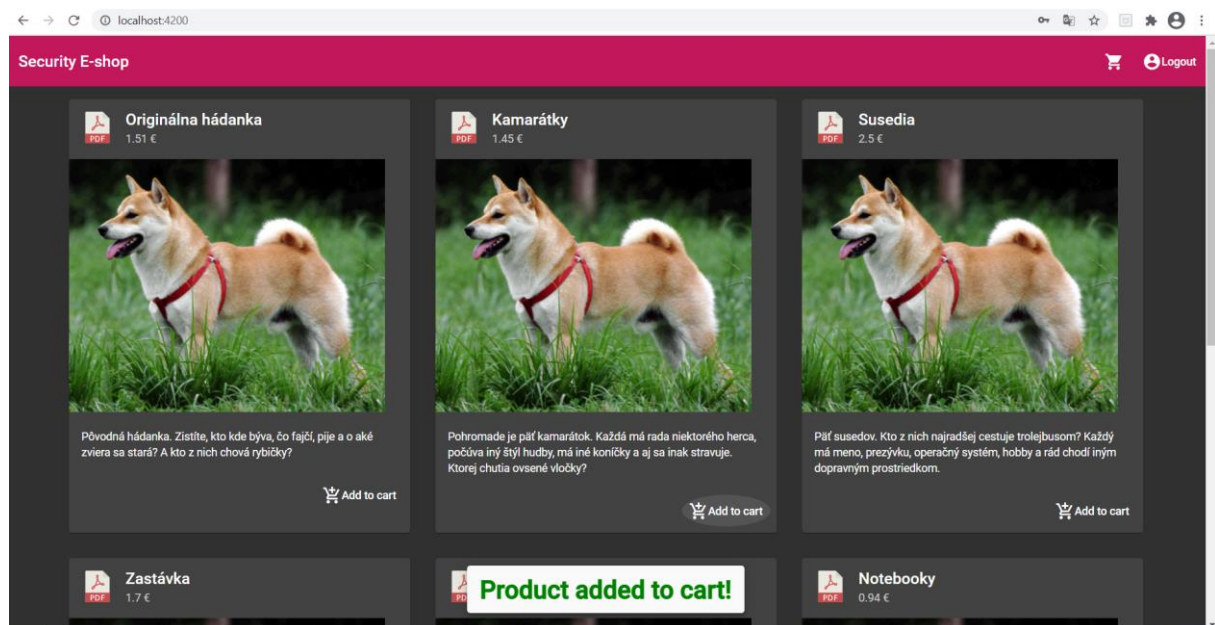
Útočník ukradne produkty z eshopu tým, že pošle vo formulári nulovú hodnotu. Najprv ale musí vytvoriť objednávku.

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



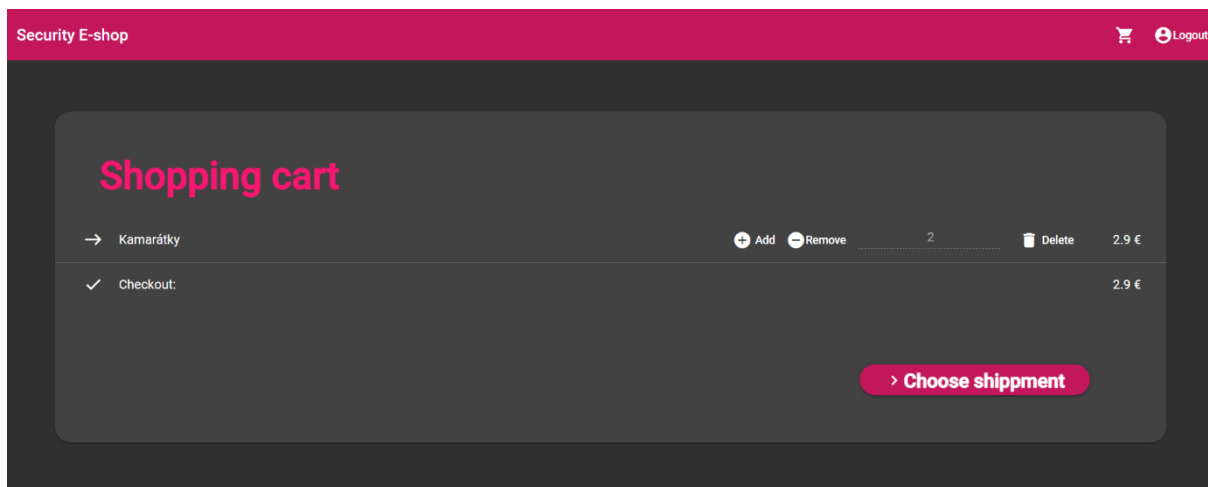
Obrázok 32: Zapnutie burpsuite a otvorenie vlastného prehliadača

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



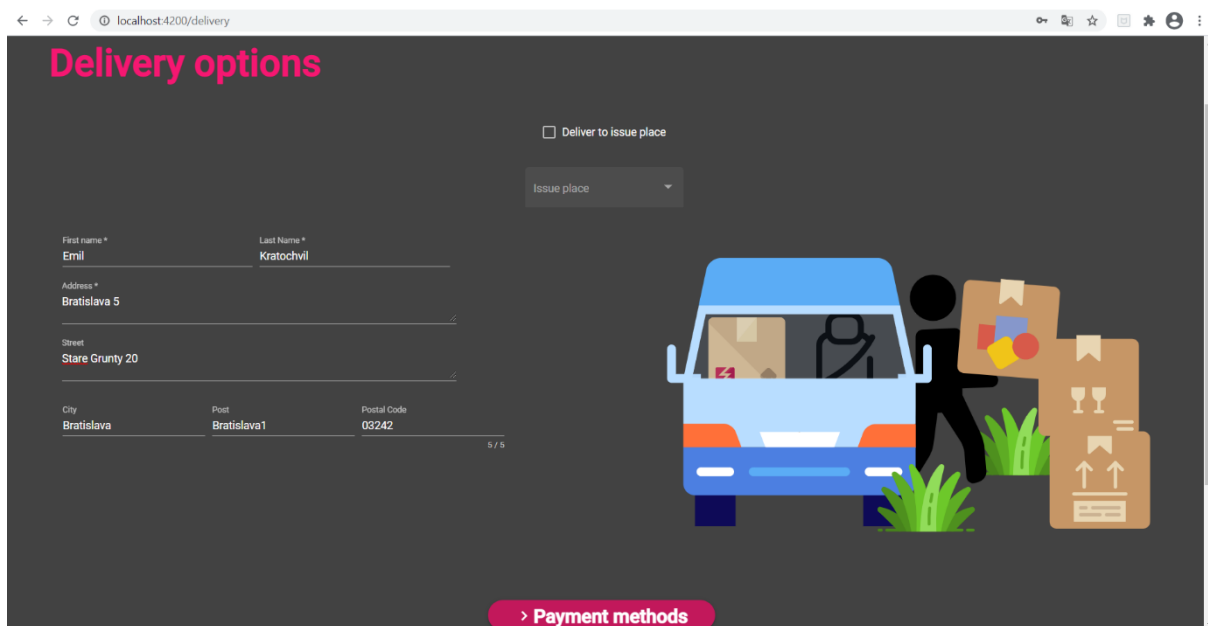
Obrázok 33: Pridanie produktu do košíka

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



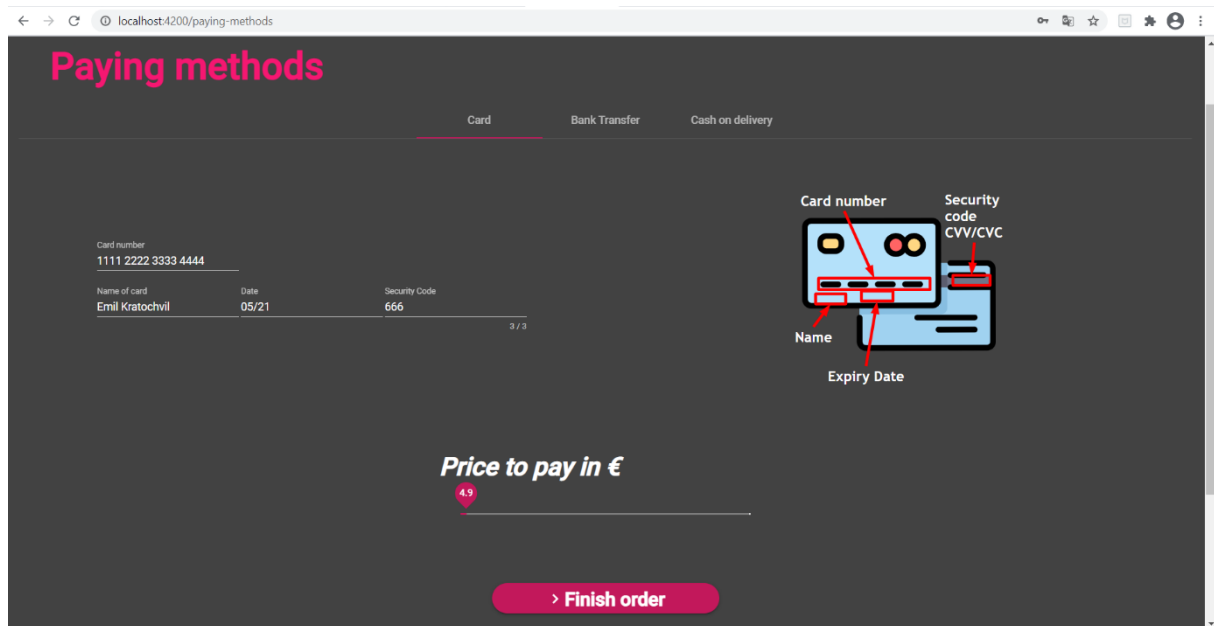
Obrázok 34: Potvrdenie produktov v košíku

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



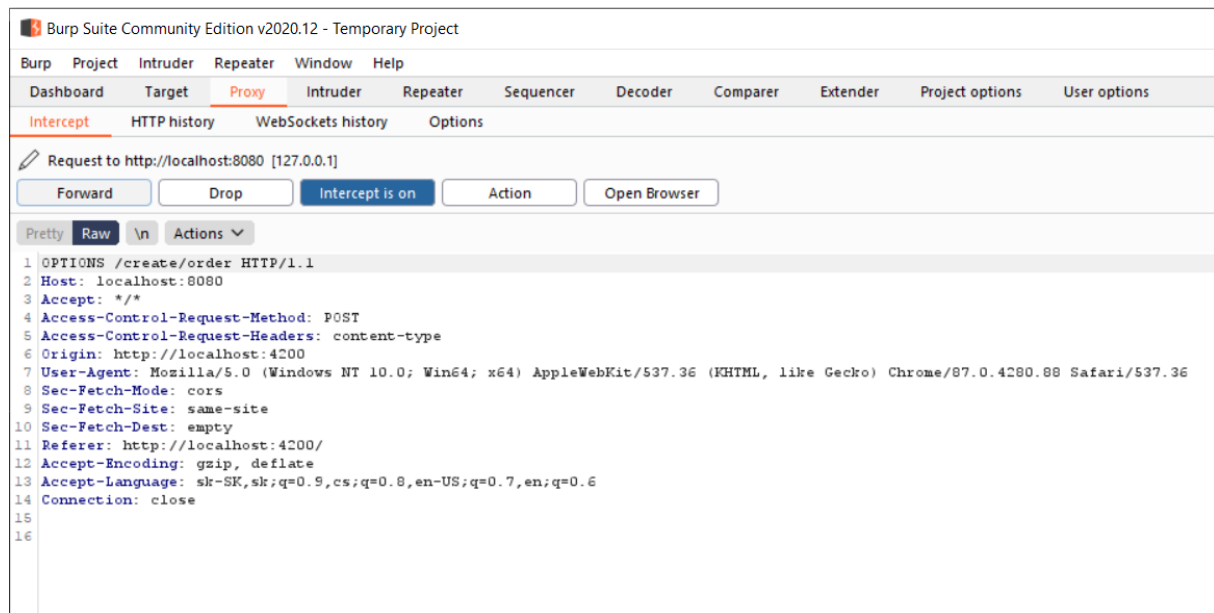
Obrázok 35: Určenie dodacej adresy

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



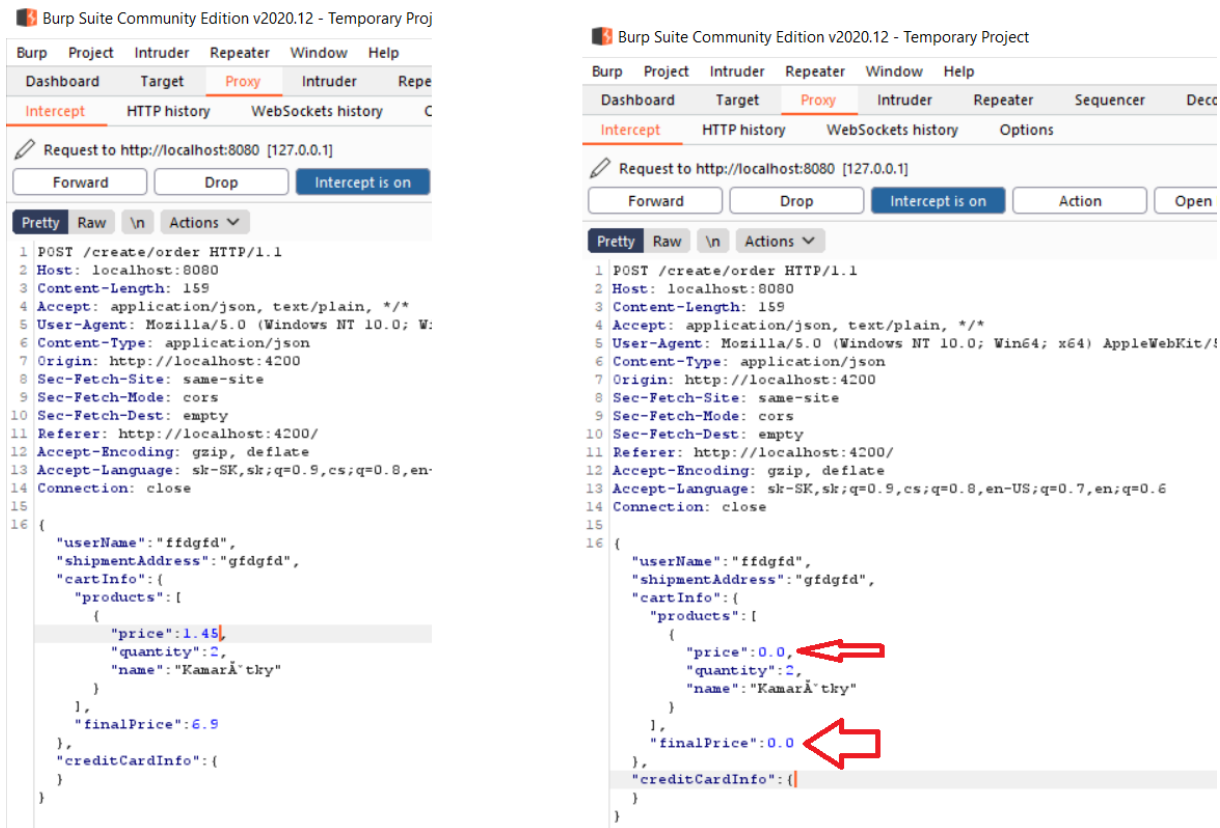
Obrázok 36: Zadanie informácií o platbe a potvrdenie

6. Prvý request prepošlite stlačením tlačidla forward.



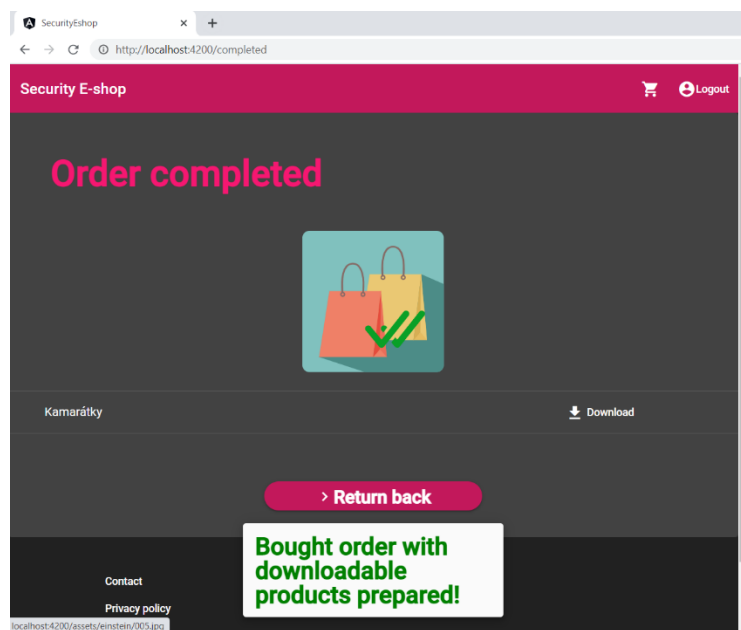
Obrázok 37: Ignorovanie prvého requestu

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



Obrázok 38: Zmena informácií v druhom requeste

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

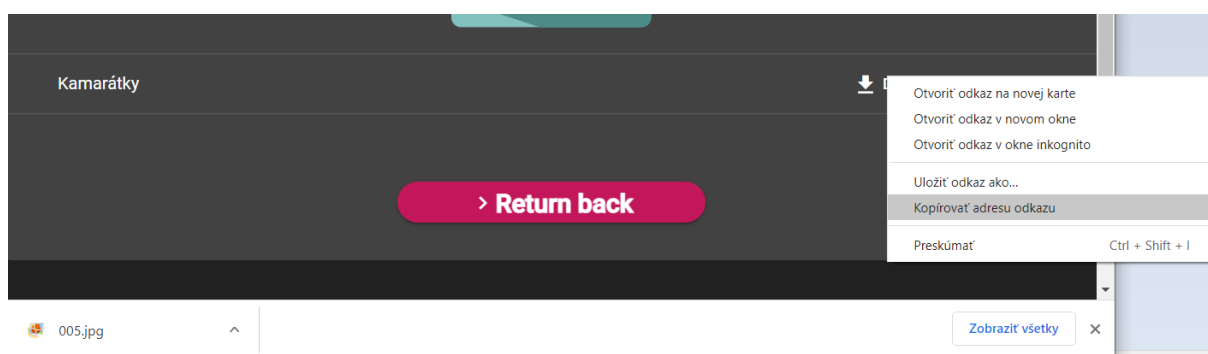


Obrázok 39: Stiahnutie ukradnutých produktov

# Získanie prístupu k súborom

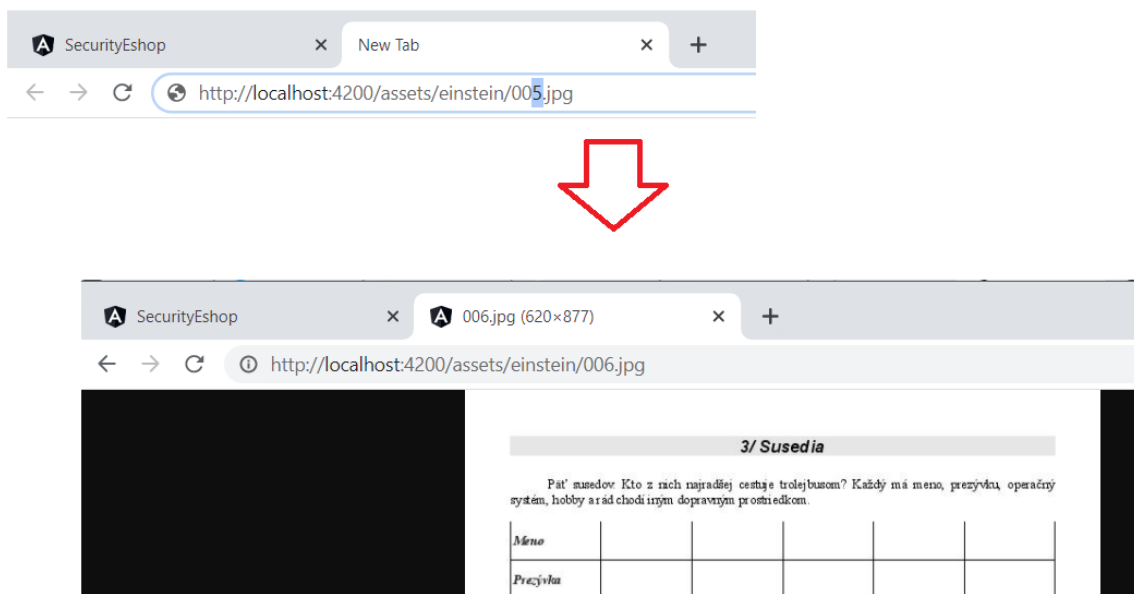
Útočník by mal vedieť, že ako technológia bol použitý Angular. Na základe tejto informácie by mal byť schopný dostať sa k verejne uloženým súborom na stránke zadáním do prehliadača cestu k assets/images. Už je len potrebné zistiť presnú cestu. Pri minulom scenári s ukradnutím produktu si ale môže všimnúť,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

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



Obrázok 41: Vyskúšanie podobnej adresy s inkrementovaným číslom obrázka