Slovenská technická univerzita v Bratislave
Fakulta informatiky a informačných technológií
Ilkovičova 2, 842 16 Bratislava 4

Používateľská príručka pre security e-shop

Tímový projekt

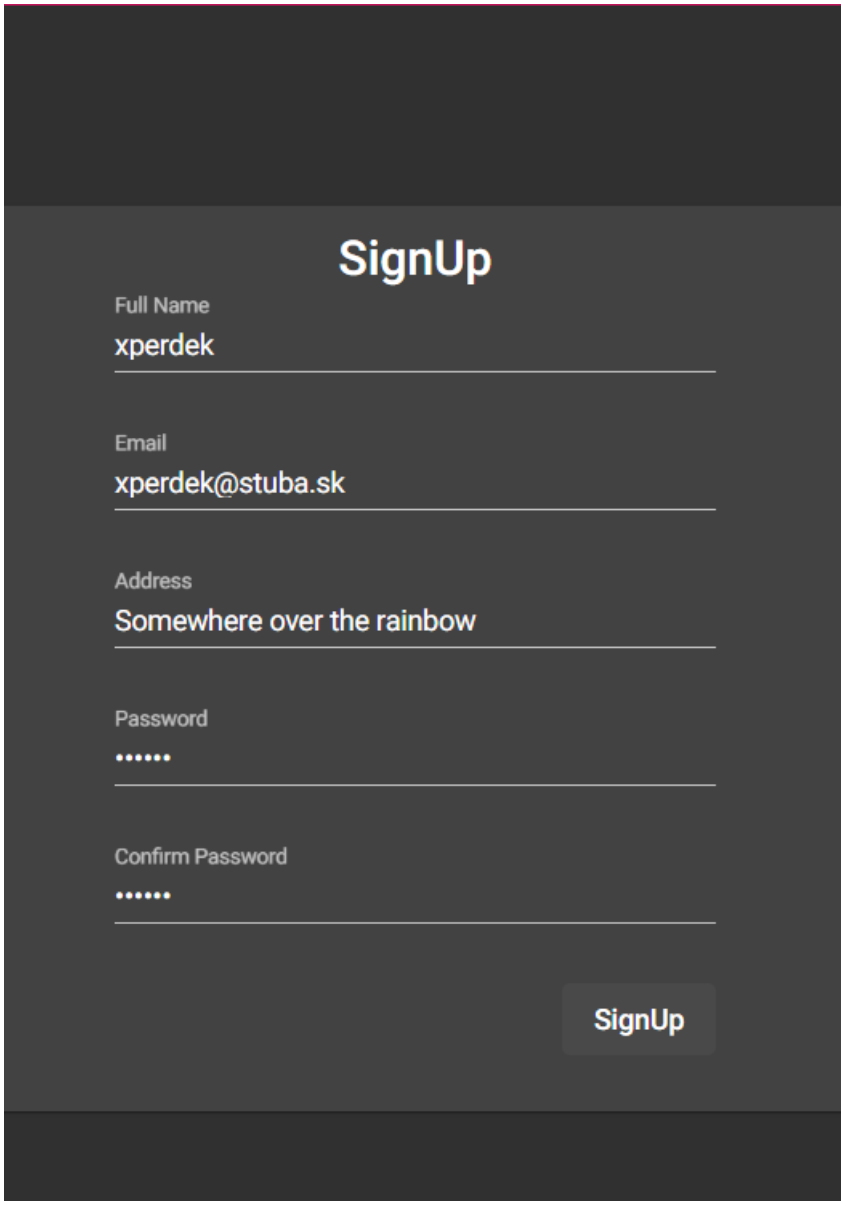
Tím č. 19

Vypracoval: Jakub Perdek
Vedúci projektu: Ing. Pavol Helebrandt Phd.

Registrácia a prihlásenie používateľa

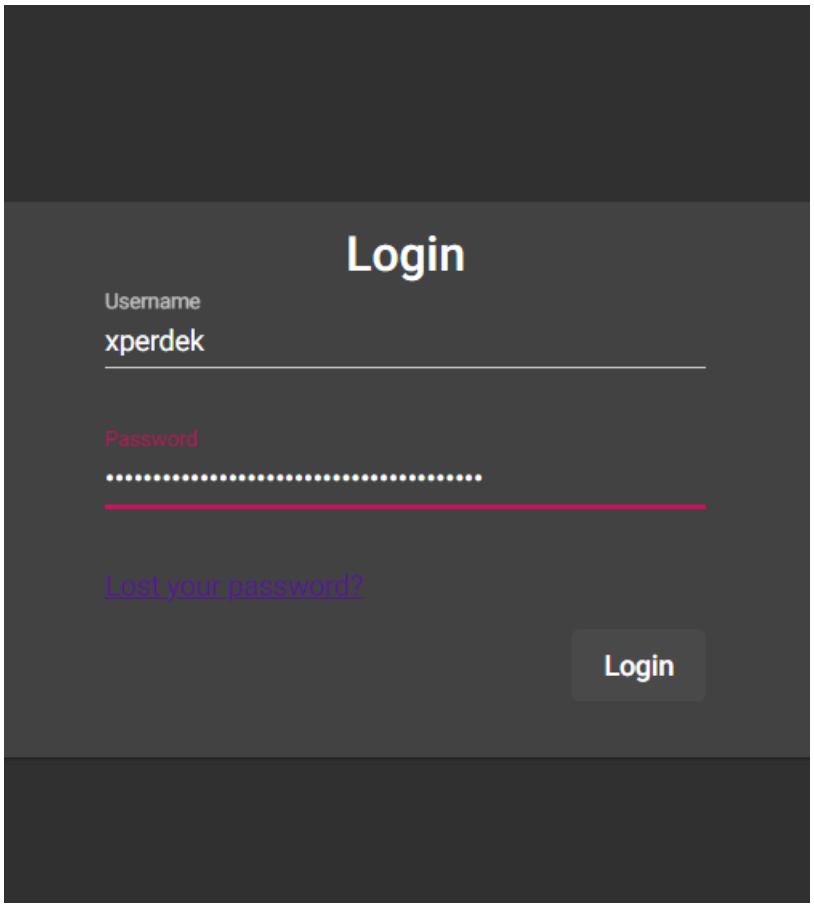
Na začiatku sa používateľ zaregistruje. Vyplní všetky položky registračného formulára. Zapamätá si meno a heslo a uvedie funkčný a jedinečný email. Následne použije meno a heslo pri prihlasovaní. Automaticky mu bude priradená roľa používateľa.

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



Obrázok 1: Registrácia používateľa

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

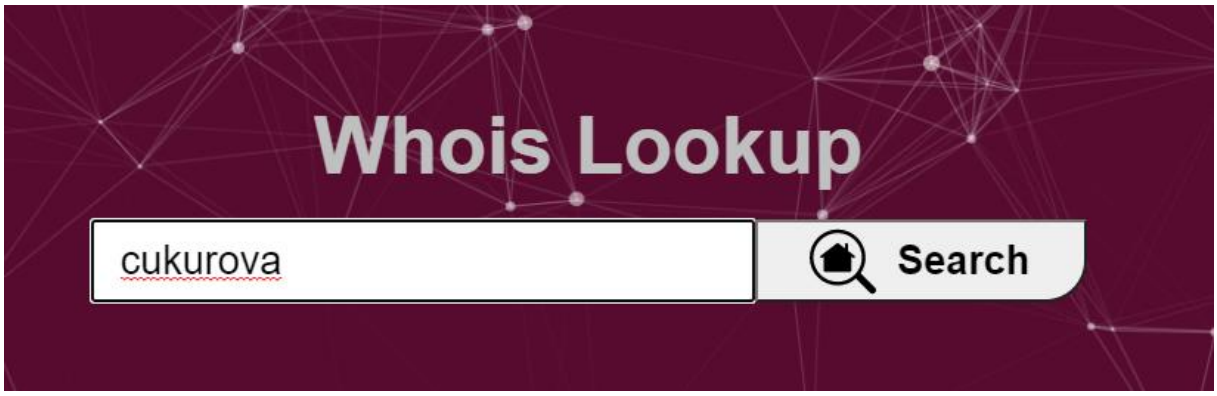


Obrázok 2: Prihlásenie používateľa

Získanie informácií o najzraniteľnejšej stránke

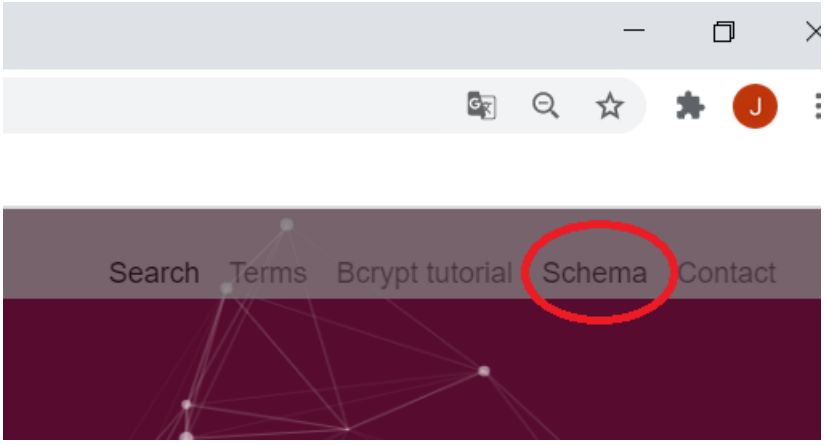
Tento scenár prezentuje pokročilú SQL injekciu. Samotné získané informácie v tomto scenári môžu uľahčiť realizáciu ďalších scenárov. Útočník sa rozhodne získať informácie z whois databázy s tým, že ho zaujíma doména s najväčším počtom zraniteľností. Vyhľadávanie mu ale vráti maximálne jednu stránku, ktorá sa najviac zhoduje s vyhľadávaným výrazom. Už asi tušíte, že potrebujete nejaký dopyt využívajúci agregačné funkcie. Našťastie Whois aplikácia poskytla schému z databázy, keďže chce prezentovať používané postupy. K potrebným informáciám sa môžete dostať na základe nasledovného postupu:

1. Otvorte whois aplikáciu dostupnú na localhost:5001
2. Zistiť ako funguje Whois môžete vyhľadaním zadaného reťazca s doménou.



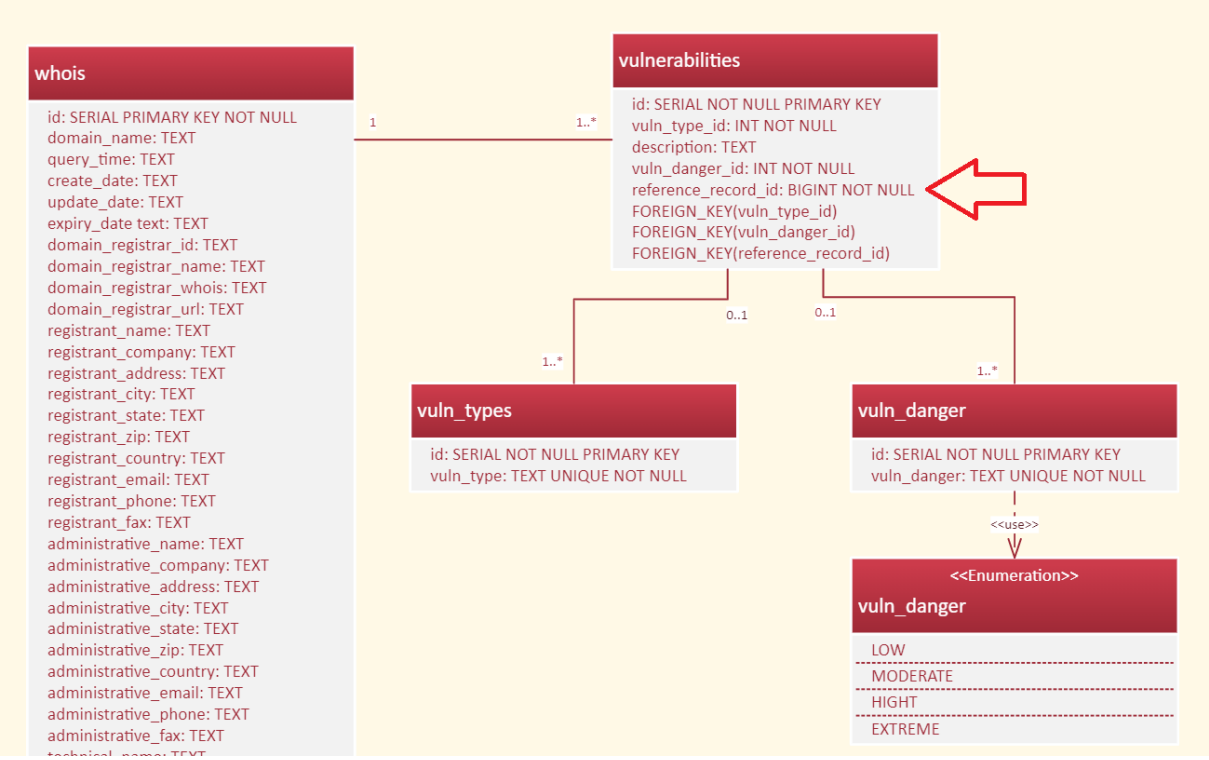
Obrázok 3: Overenie funkcionality whois

3. Následne sa presmerujte na stránku s dátovým modelom whois



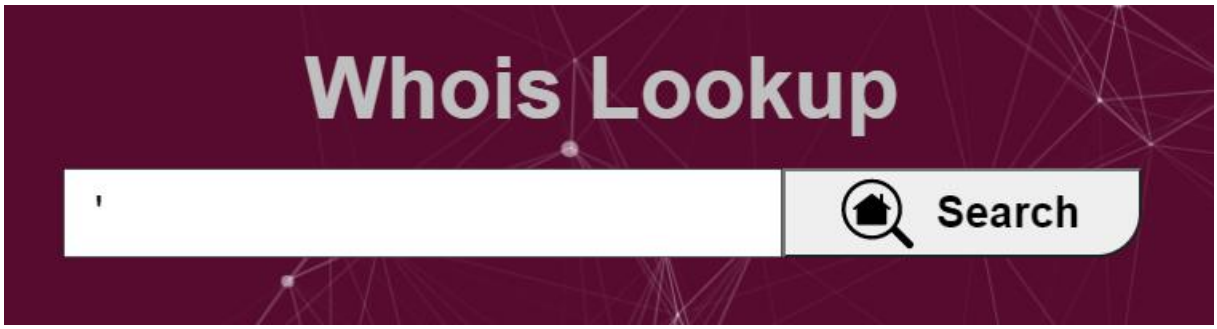
Obrázok 4: Presmerovanie sa na stránku s whois schémou

4. V menu zvoľte Schema. Dostali ste sa na stránku s databázovou schémou. Zo schémy môžete zistiť, že whois tabuľka so záznamami z ktorých sa vyhľadáva sú prepojené s tabuľkou zraniteľností pomocou cudzieho kľúča reference record id.



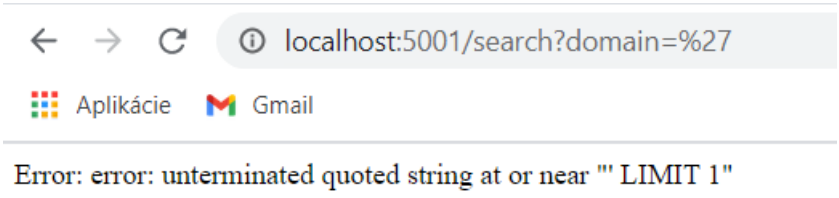
Obrázok 5: Databázová schéma aplikácie Whois

5. Teraz už viete, čo môžete pri písaní SQL injekcie využiť. Ešte je potrebné overiť, či injekcia bude fungovať. Presmerujte sa preto na úvodnú stránku s vyhľadávačom.
6. Zadajte do okna ‘ a potvrďte. V špeciálnych prípadoch môže byť ochrana vo formulároch na frontende. Pokiaľ by bola bolo by potrebné použiť na odosielanie requestov BurpSuite. Jeho použitie si ukážeme v ďalších scenároch.



Obrázok 6: Overenie, či SQL injekcia bude fungovať

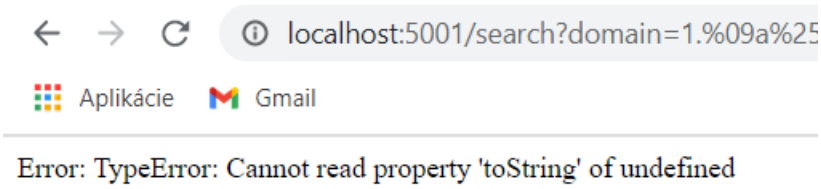
7. Zobrazila sa vám chybová hláška, na základe ktorej viete, že prípadná SQL injekcia bude úspešná.



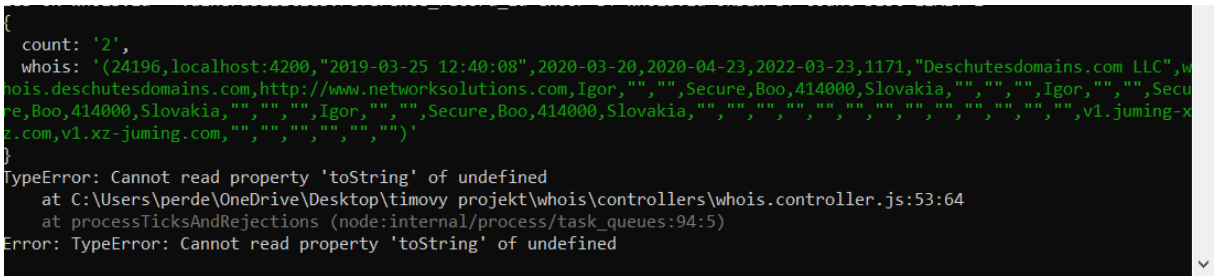
Obrázok 7: Chybové hlásenie zobrazujúce neošetrenú slabinu v systéme

8. Konečne môžete navrhnúť SQL injekciu. Najprv je potrebné zistiť ako funguje vyhľadávanie na základe reťazca. Keďže slovo je hľadané kdekoľvej v doméne potom možno usúdiť, že v postgrese je výraz ohraničený a vyzerá nasledovne: '%vyhladavana_domena%'
   Preto je potrebné najprv uzatvoriť predtým vyhľadávaný reťazec a zároveň zabezpečiť, aby podmienka pre akýkoľvek platila, napríklad použitím logického OR a výrazu, ktorý bude vždy pravdivý.
   Zatiaľ sme navrhli výraz: a%' OR 1=1
   Ten je potrebné ešte okomentovať a vložiť pred komentár ohraničenie pre vrátenie práve jedného výsledku, lebo v kóde sa vracia najviac jeden vyhľadaný a pravdepodobne sa volá funkcia one. Ak by bolo vrátených viac výsledkov skončí s chybou. Pridáme preto na koniec reťazec LIMIT 1 --'
   Zatiaľ máme: a%' OR 1=1 LIMIT 1 --'
9. Môžete skúsiť použiť výraz a%' OR 1=1 LIMIT 1 --' vo vyhľadávaní. Vidíte, že bez chyby vráti nejaký výsledok. Vy ale chcete aby bo, vrátený výsledok s najväčším počtom zraniteľností.
10. Do reťazca doplňte agregačný dopyt na základe ktorého bude možné získať potrebné výsledky. Vyžite informácie zo schémy Whois aplikácie. Keby sme mali prístup k database napísali by sme takýto SELECT:
    SELECT
    COUNT (vulnerabilities.reference_record_id) AS count, whois AS whois
    FROM whois
    LEFT JOIN vulnerabilities ON whois.id = vulnerabilities.reference_record_id
    GROUP BY whois.id
    ORDER BY count DESC
    LIMIT 1
    Týmto selectom na základe agregačnej funkcie COUNT spočítame záznamy pre cudzí kľúč záznamu zraniteľnosti odkazujúci na whois záznam. Čím je tento poćet vyšší, tým viac záznamov o zraniteľnostiach pre konkrétny whois záznam existuje. Netreba zabudnúť spojiť tabuľku so zraniteľnosťami a whois tabuľku so záznamami LEFT JOINOM. Opäť je potrebný výber práve jedného záznamu pomocou LIMIT 1. Chceme najvyššiu hodnotu preto zoradíme výsledky zostupne pomocou ORDER BY count DESC, kde count je agregovaný počet pre každú jedinečnú hodnotu cudzieho kľúča, respektíve identifikátor whois zánamu.

11. Navrhnutý agregačný dopyt skombinujte pridaním bodkočiarky za výraz 1=1 a jeho doplnením za túto bodkočiarku.
    V tomto kroku by sme mali mať:
    a%' OR 1=1; SELECT COUNT(vulnerabilities.reference_record_id) AS count, whois AS whois FROM whois LEFT JOIN vulnerabilities ON whois.id = vulnerabilities.reference_record_id GROUP BY whois.id ORDER BY count DESC LIMIT 1 --'
    Skúste tento výraz vložiť do vyhľadávacieho okno.
12. Dostali ste chybovú hlášku, kde sa program sťažuje, že niektorá hodnota je undefined. Pri simulovaní situácie s použitím podobnej node js aplikácie alebo po hlbšej úvahe by ste mohli zistiť, že hodnoty sa nevrátia ako slovník.



13. **Obrázok 8: Chyba pri vyskúšaní pripravenej injekcie**



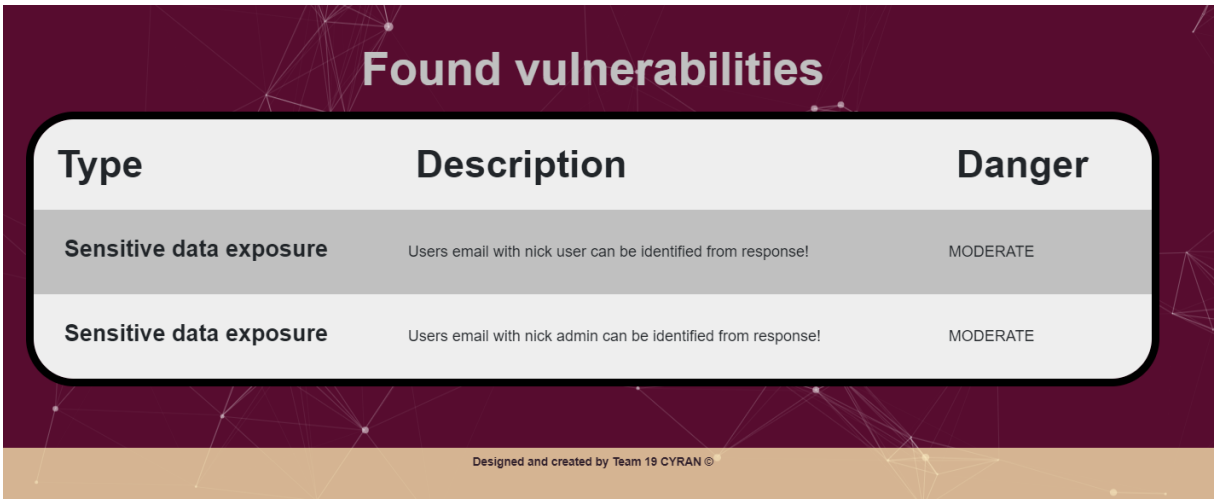
Obrázok 9: Hodnoty záznamu sa nevrátia ako slovník

Obrázok 10: Podoba dát keby boli slovníkom

14. Upravte preto príkaz tak, aby bol vrátený len id hľadaného záznamu teraz už bez ďalších JOIN operácií, tak aby vrátilo slovník. Výraz by mal fungovať. Postup je nasledovný.

V predchádzajúcom agregačnom dopyte zmeňte vrátený výsledok z whois záznamu len na id whois záznamu:
SELECT
COUNT (vulnerabilities.reference_record_id) AS count, whois**.id** AS **ww**
FROM whois
LEFT JOIN vulnerabilities ON whois.id = vulnerabilities.reference_record_id
GROUP BY whois.id
ORDER BY count DESC
LIMIT 1
Celý výraz po vložení vyzerá nasledovne:
a%' OR 1=1; SELECT COUNT(vulnerabilities.reference_record_id) AS count, whois**.id** AS **ww** FROM whois LEFT JOIN vulnerabilities ON whois.id = vulnerabilities.reference_record_id GROUP BY whois.id ORDER BY count DESC LIMIT 1 --'

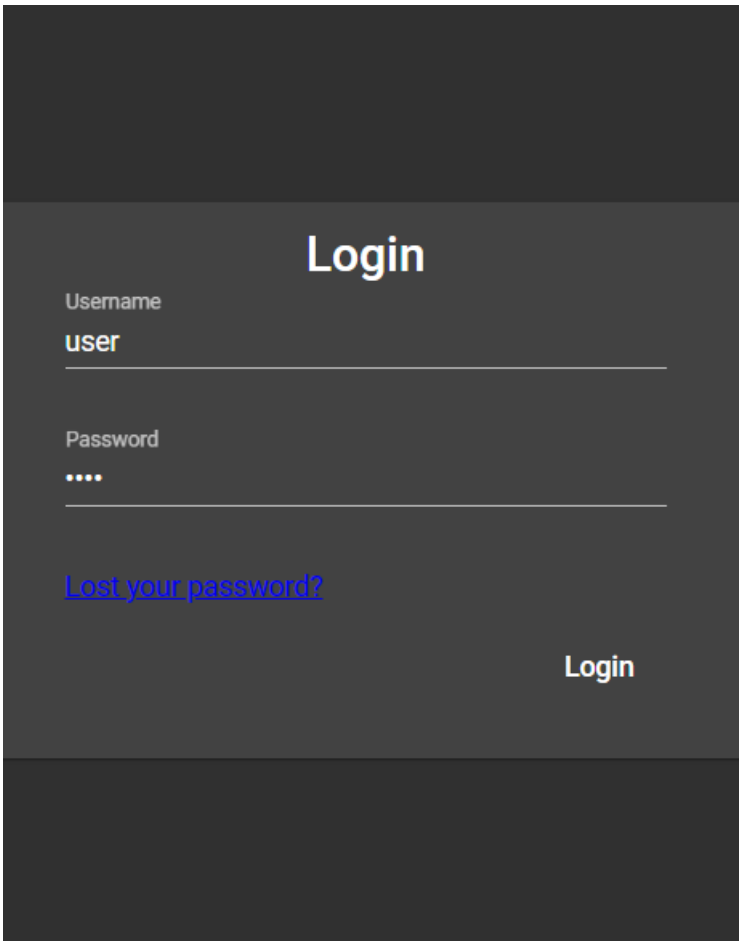
15. Pridajte ďalší SELECT do tohto agregovaného dopytu dopytujúceho sa do tabuľy whois po zázname na základe získaného id z dopytu:
a%' OR 1=1; **SELECT * FROM whois, (**SELECT COUNT(vulnerabilities.reference_record_id) AS count, whois.id AS ww FROM whois LEFT JOIN vulnerabilities ON whois.id = vulnerabilities.reference_record_id GROUP BY whois.id ORDER BY count DESC LIMIT 1**) ww WHERE ww = whois.id** LIMIT 1 --'
16. Následne ho overte pri vyhľadávaní. Získali ste záznam s dvomi zraniteľnosťami. Asi nie je prekvapením, že odkazujú na security eshop. Zo záznamov ste sa mohli dozvedieť mená dvoch významných používateľov eshopu, ktoré sa zídu v ďalších scenároch.



Obrázok 11: Získané zraniteľnosti pre doménu s najväčším počtom zraniteľností

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.

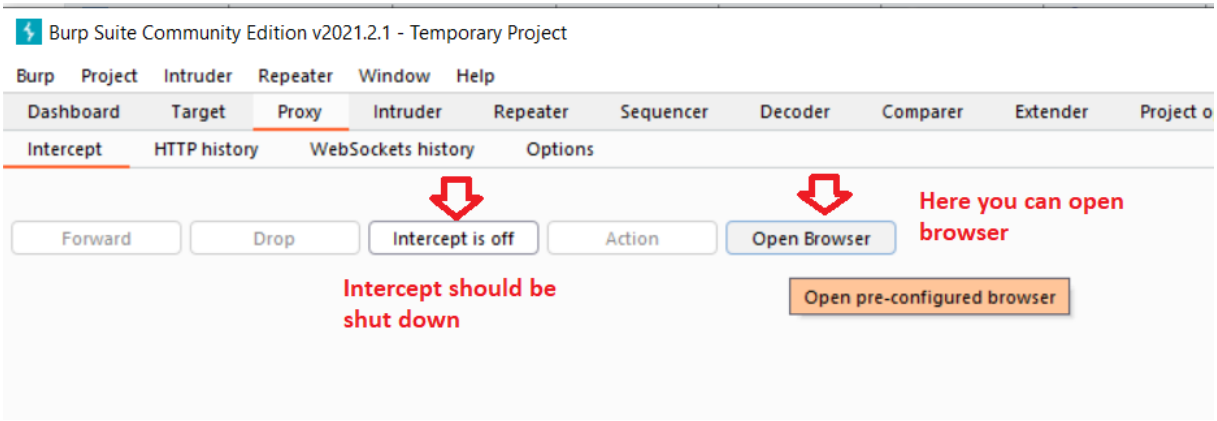


Obrázok 12: Aplikovanie jednoduchého hesla user

Prelamovanie hesiel slovníkovým útokom

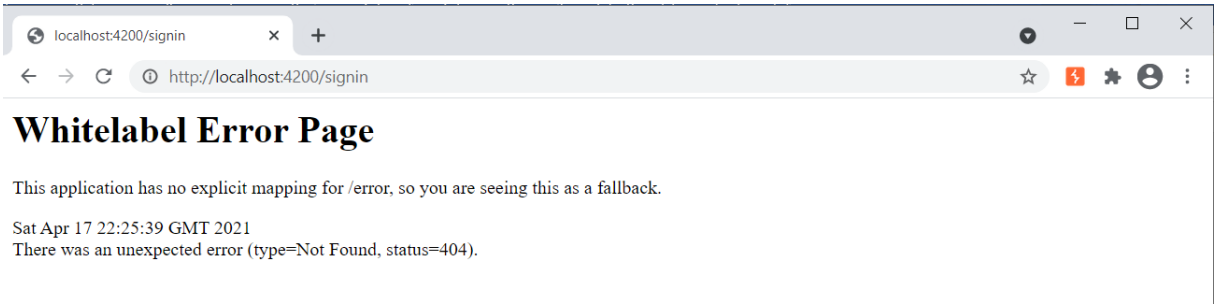
Útočník môže zrealizovať slovníkový útok na základe získaných informácií z login stránky. K užitočným informáciám sa dostanete na základe nasledujúceho postupu:

17. Po zapnutí burpsuitu a prejdite do kolónky proxy.
18. Vypnite intercept v rozkliknutom menu BurpSuite.
19. Otvorte si prehliadač kliknutím na open browser.



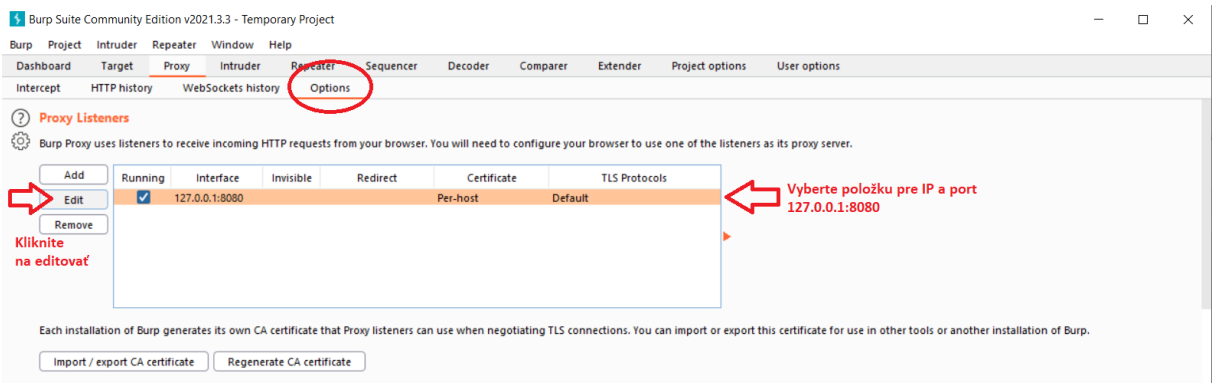
Obrázok 13: Otvorenie prehliadača a interceptor v BurpSuite

20. Prejdite na stránku http://localhost:4200/signin.
21. Ak sa vám zobrazí chyba ako na obrázku 5 postupujete podľa ďalších krokov. Ak vám všetko funguje pokračujte krokom 8.



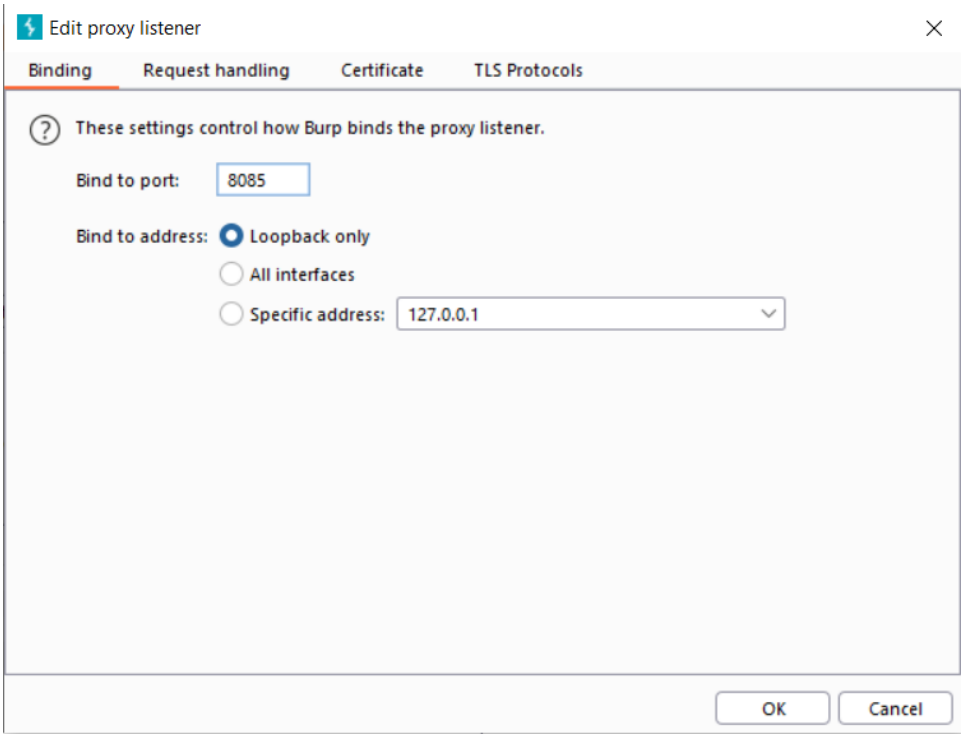
Obrázok 14: Chyba v zabudovanom prehliadači pre BurpSuite

22. V burpsuite si na lište vo vybranej kolónke proxy rozkliknite tab Options. V časti Listeners zvoľte záznam pre localhost s IP 127.0.0.1 a kliknite na editovať.



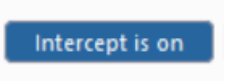
Obrázok 15: Zmena nastavenia proxy

23. Následne zmeňte port z 8080 napríklad na 8085. Overte či obsah v prehliadači funguje. Ak áno pokračujte nasledovným bodom.



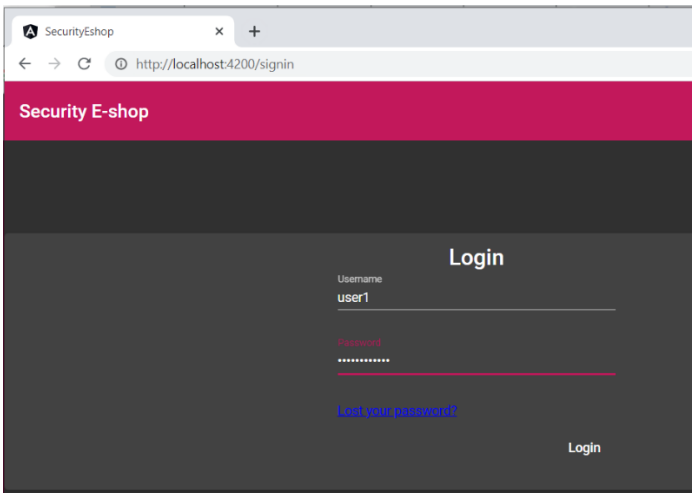
Obrázok 16: Zmena portu

24. Zapnite intercept na tej istej položke v menu BurpSuite.



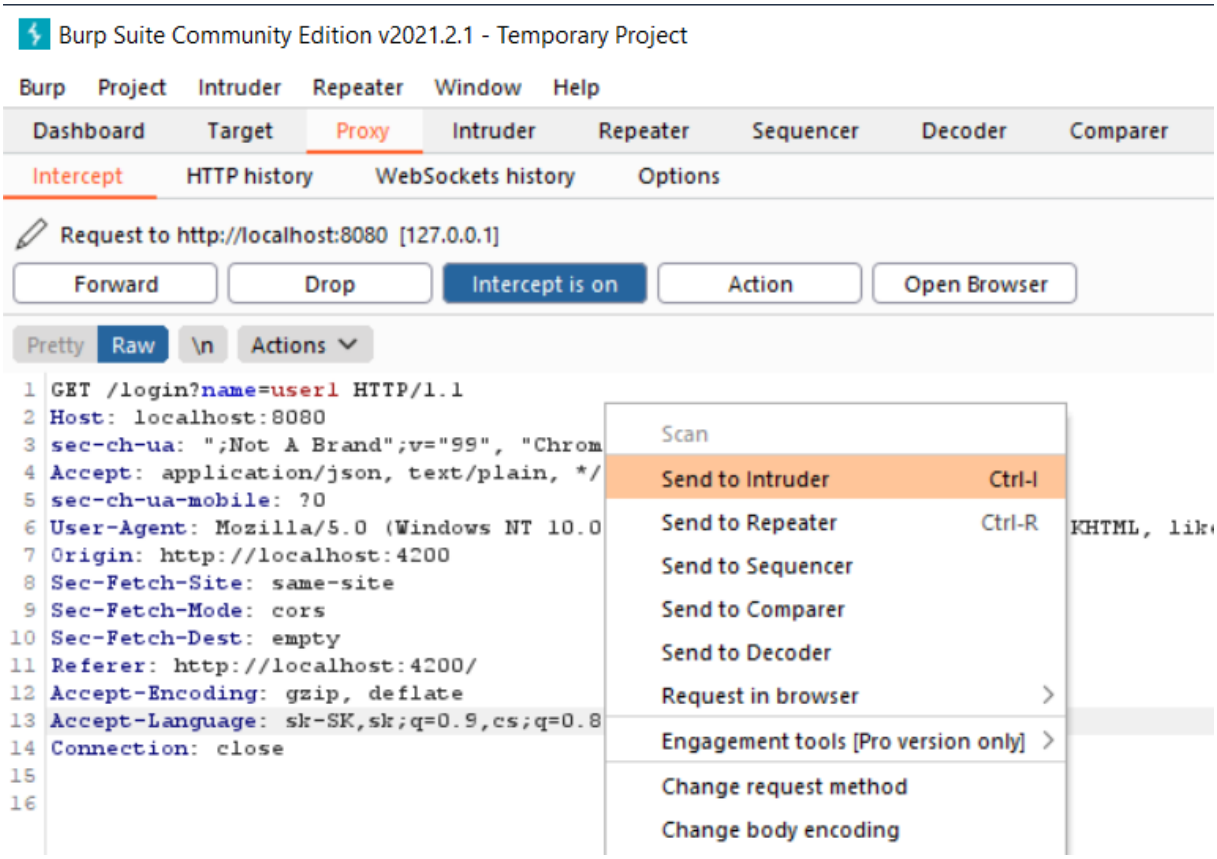
Obrázok 17: Zapnutie interceptora

25. Pokúste sa prihlásiť s ľubovoľným menom a heslom.



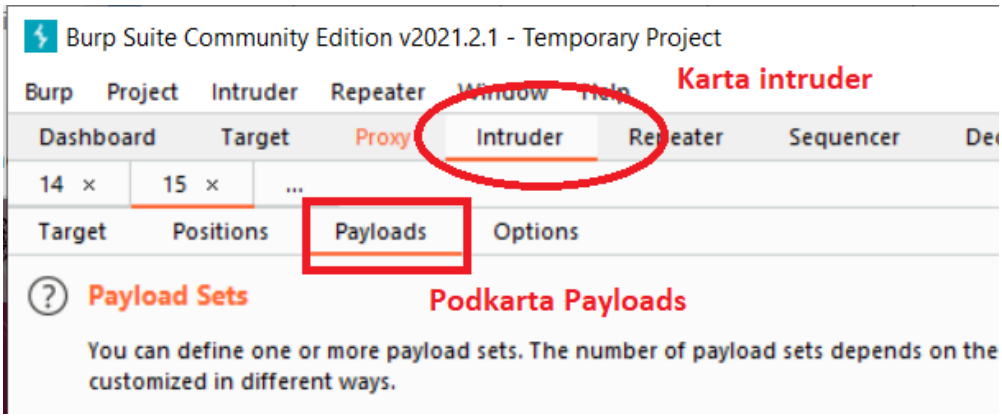
Obrázok 18: Pokus o prihlásenie v stavanom prehlaidači BurpSuitu

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



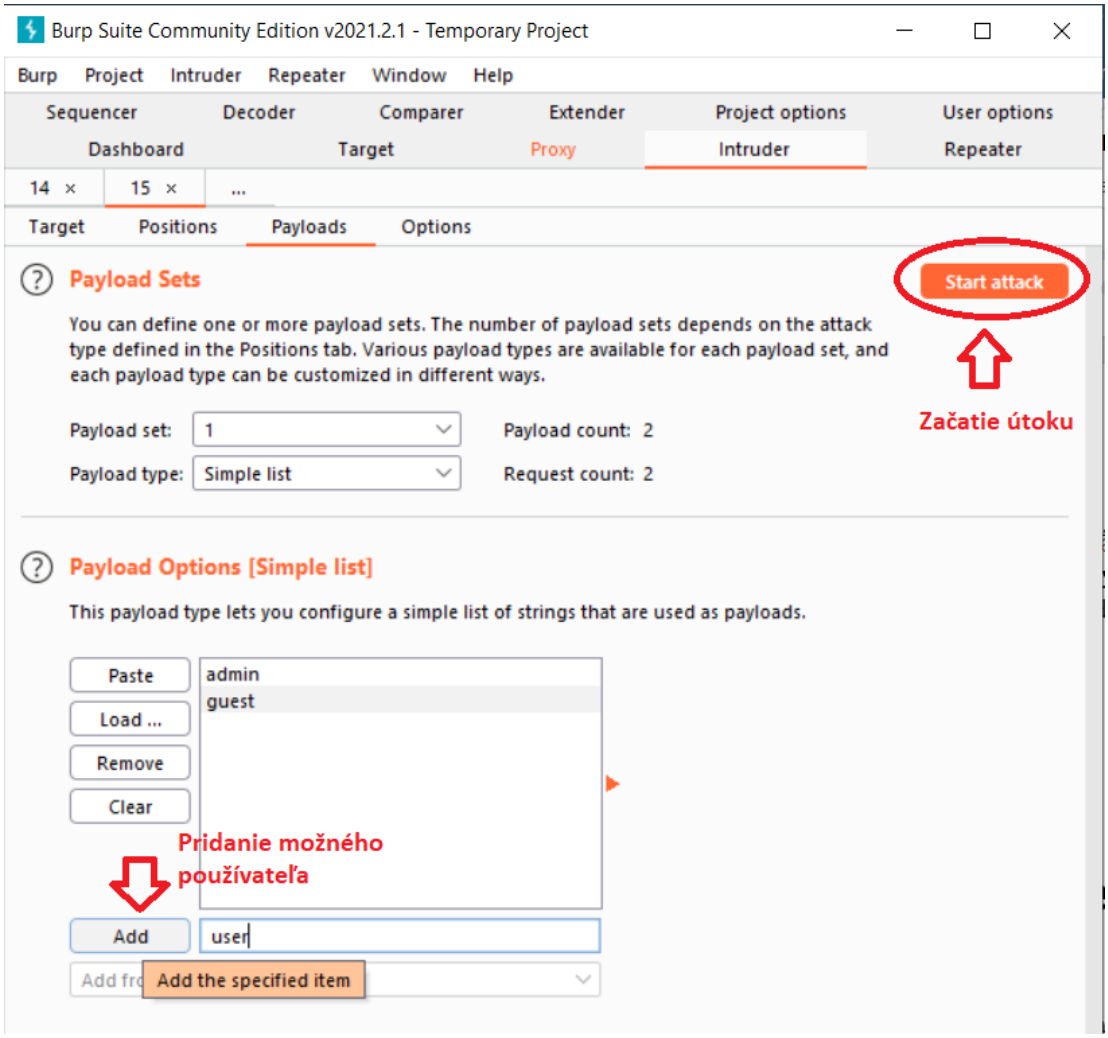
Obrázok 19: Odoslanie requestu do intrudera

29. Následne kliknite na otvorenú položku Intruder-a.
30. Rozkliknite podmenu Payloads v položke Intruder-a.



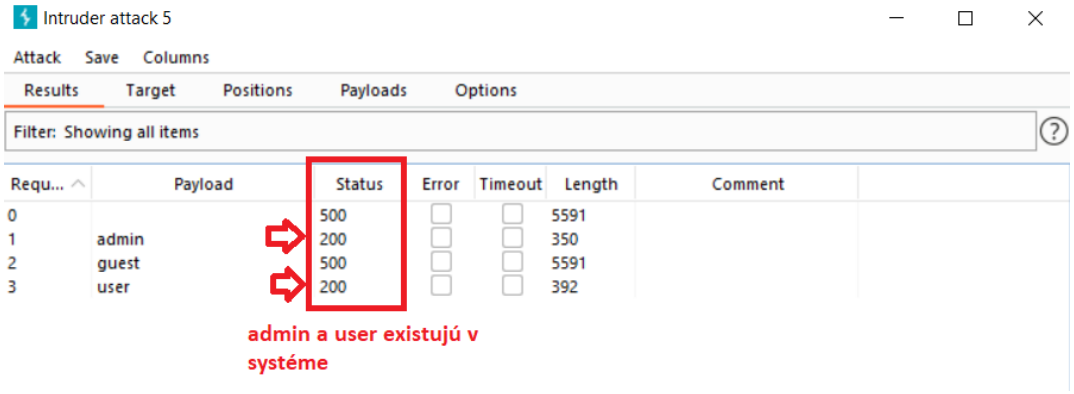
Obrázok 20: Presunutie sa na položku Payloads v Intruderovi

31. Vo vrchnej časti Payload Sets rozkliknutej karty v BurpSuite nechajte nastavené Payload set na 1 a Payload type na Simple list.
32. 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.
33. Zvoľte položku "Start attack".



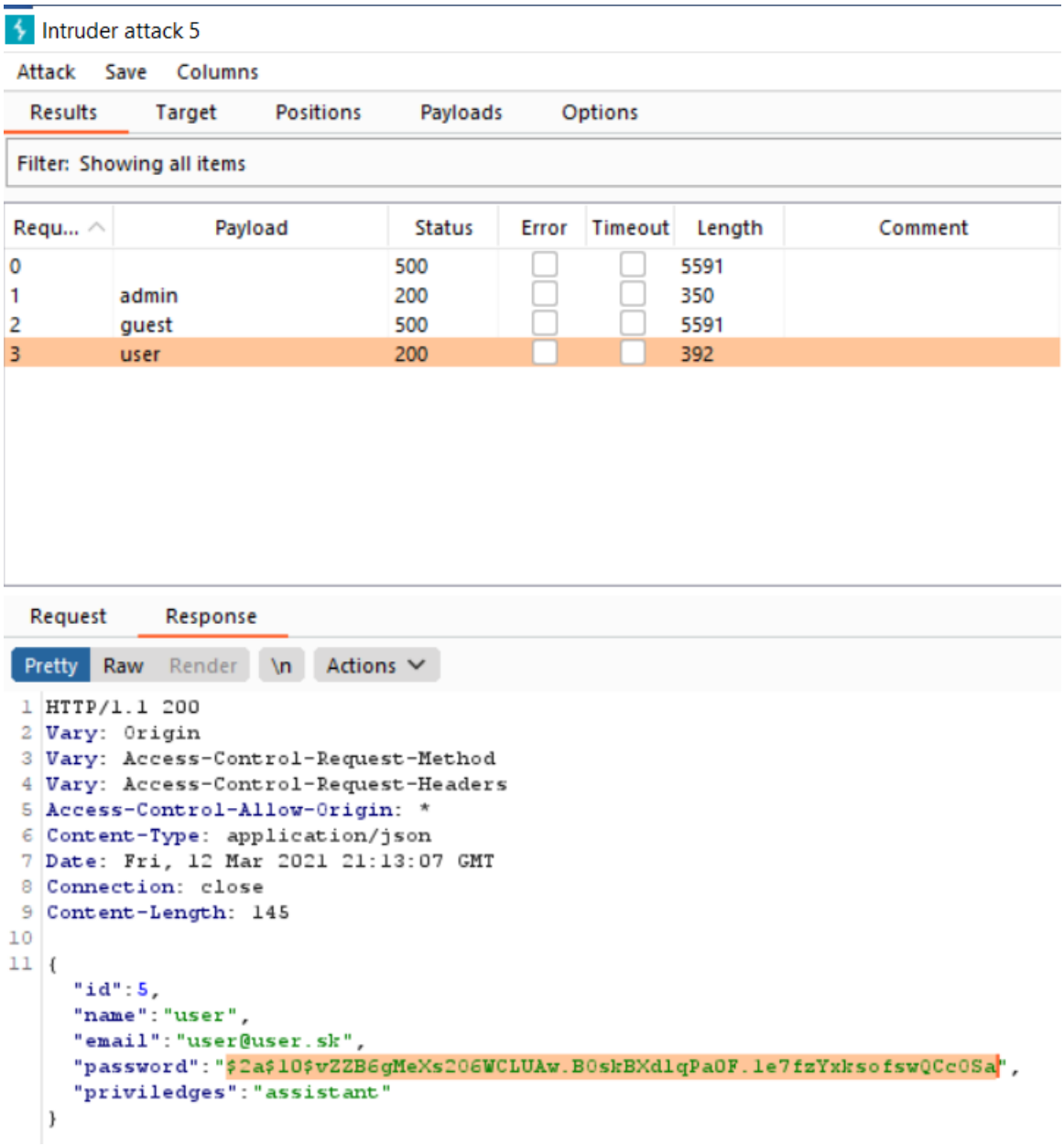
Obrázok 21: Zadanie zoznamu potencionálnych používateľov a začatie útoku

34. Otvorí sa okno, v ktorom podľa vráteného statusu môžte zistíť, ktorí používatelia existujú v systéme.
35. Kliknite na jeden z riadkov, ktorý má status 200.
36. Prepnite sa na kartu Response, v okne ktoré sa zobrazí nižšie.
37. 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 22: Zistenie existujúcich používateľov v systéme

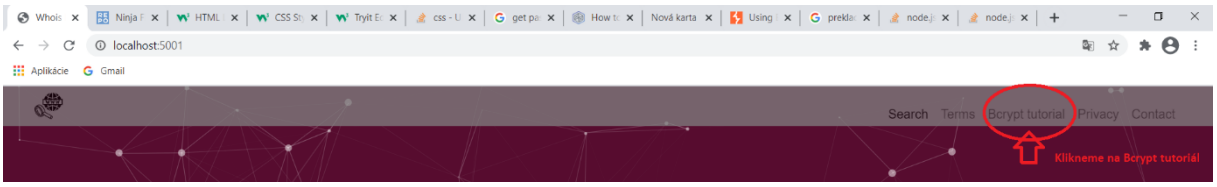
38. Skopírujte heslo usera, ktorý je asistent.



Obrázok 23: Získanie zašifrovaného hesla asistenta s používateľským menom user

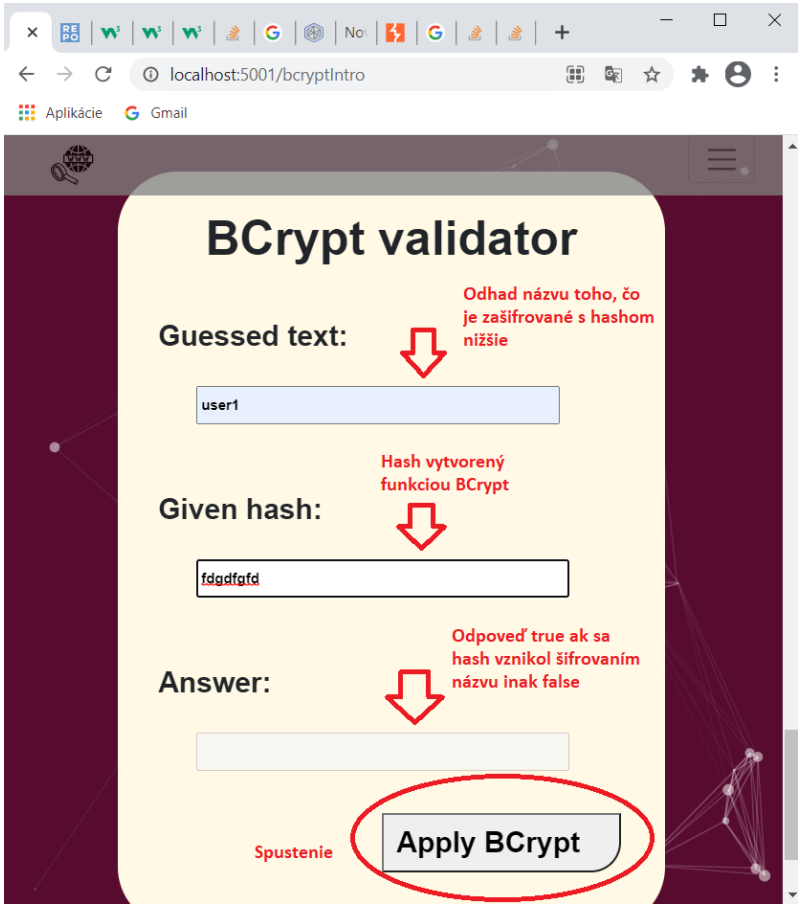
Získali ste heslo, ale je ho potrebné ešte prelomiť. Z Whois aplikácie, prezretím zdrojového kódu projektu, alebo vďaka nejakej nápovede by ste mali vedieť, že na šifrovanie bol použitý bcrypt v javascripte. Je teda potrebné overiť množinu možných hesiel voči tomuto hashu. Skúsite ich preto overiť použitím 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/.
4. V ľavom hornom rohu kliknite na položku v menu s názvom “Bcrypt tutorial”.



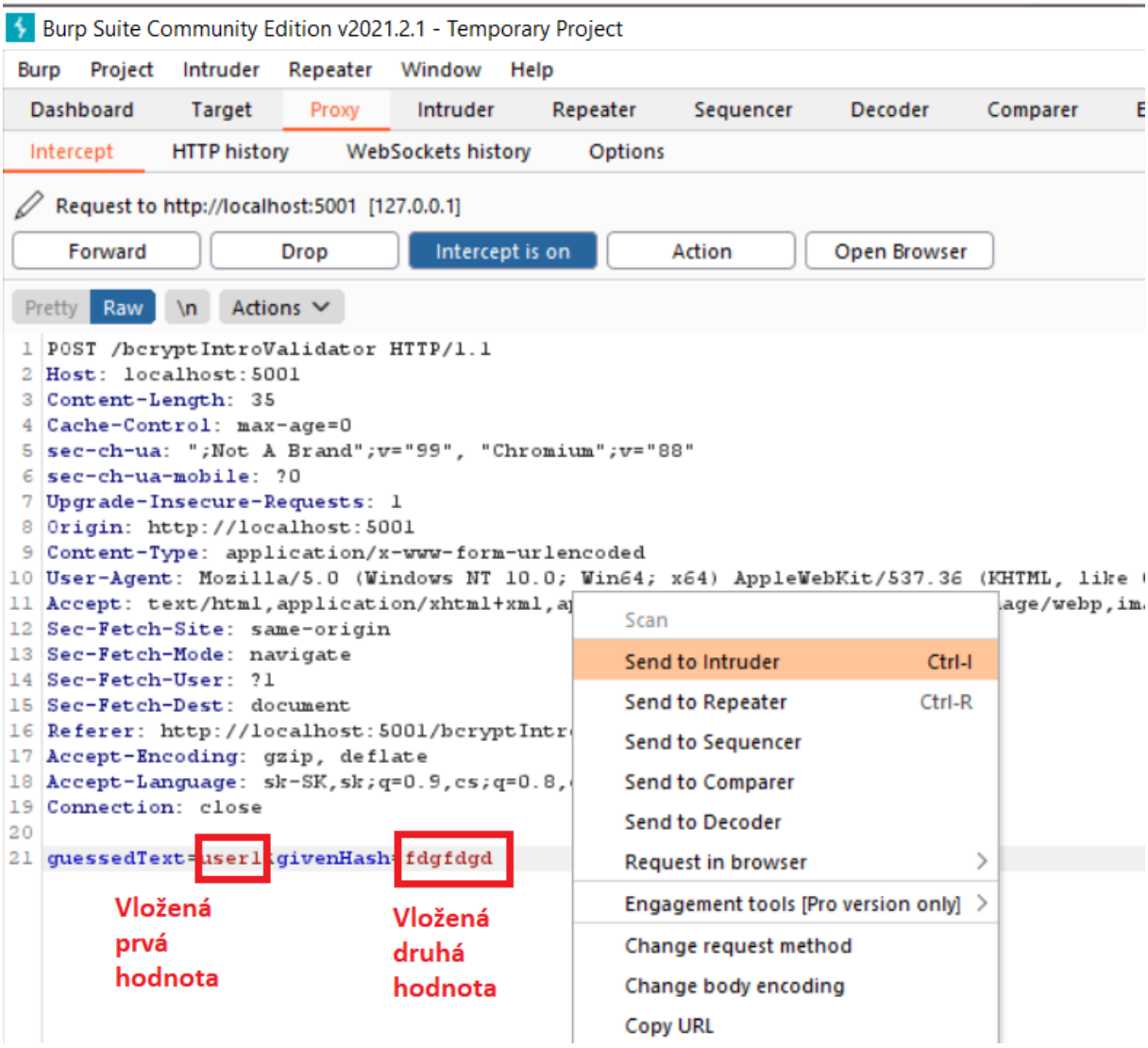
Obrázok 24: Vyhľadanie stránky s tutoriálom pre Bcrypt

5. Preskrolujte na službu s názvom BCrypt validator.



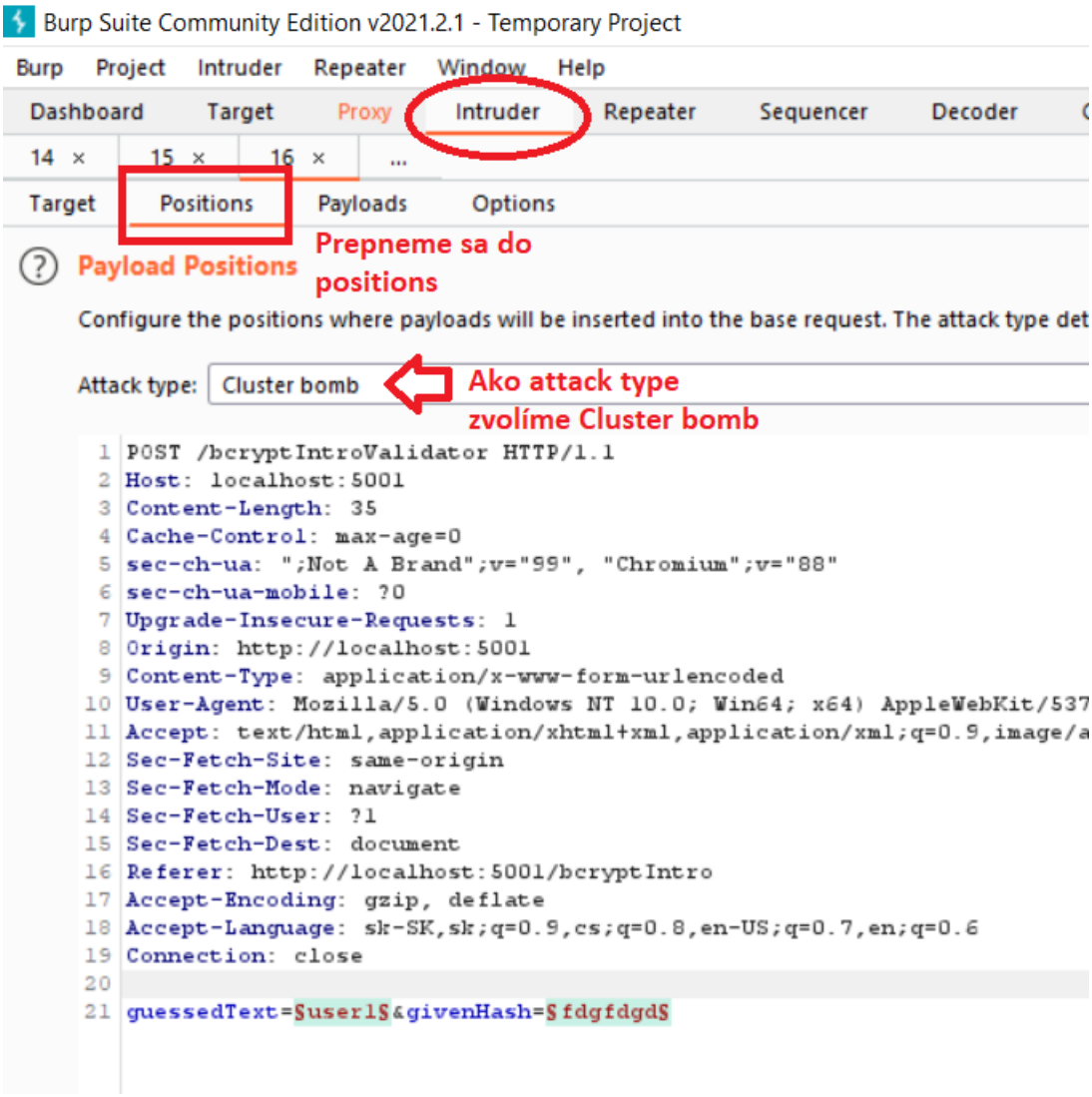
Obrázok 25: Vyvolanie služby pre zistenie či hash vznikol šifrovaním odhadovaného textu

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.



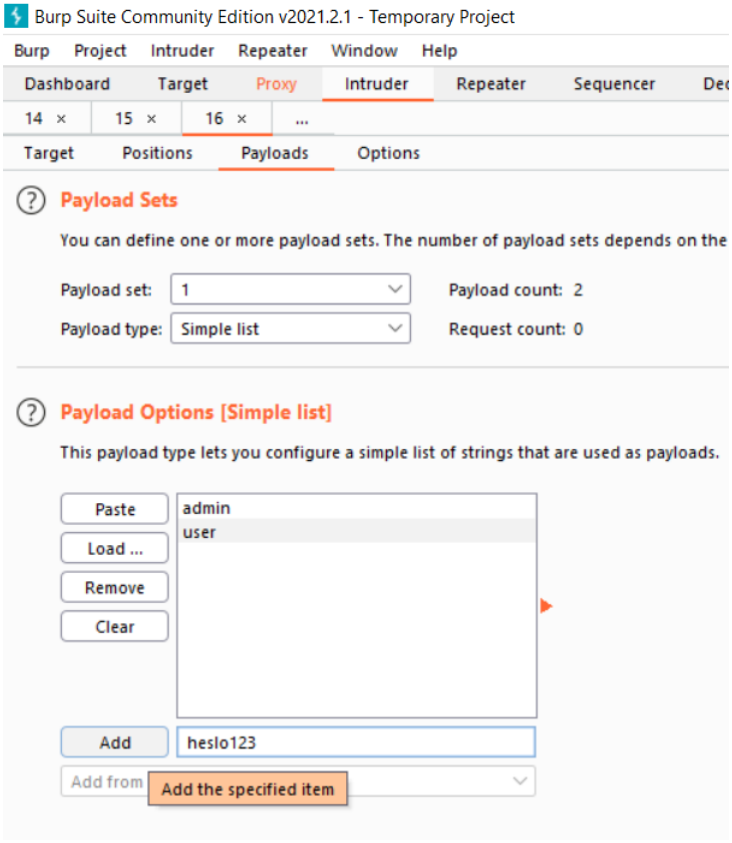
Obrázok 26: Zachytená odoslaná žiadosť na server a odoslanie do intrudera

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

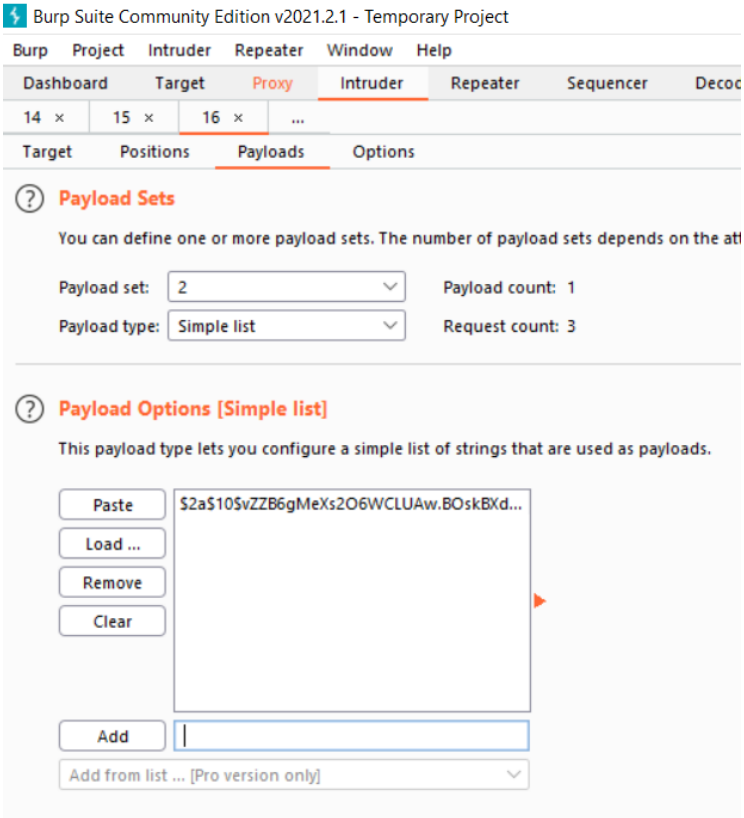


Obrázok 27: Nastavenie typu útoku na Cluster bomb

11. Následne sa prepnite do podmenu karty Intruder s názvom Payloads.
12. 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.
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. Prepnite 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.

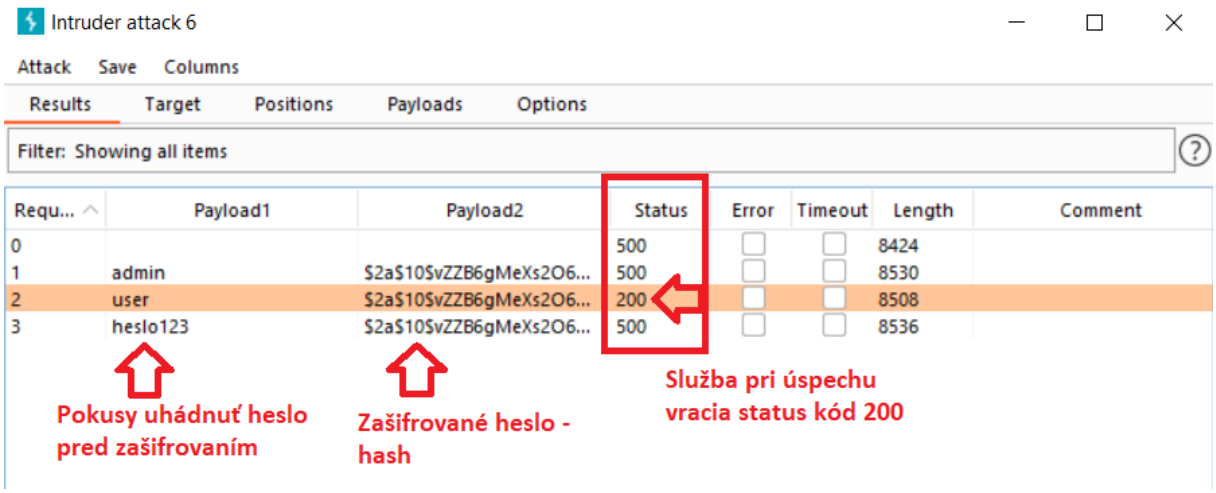


Obrázok 28: Zadanie potencionálnych odhadovaných hesiel – nešifrovaných



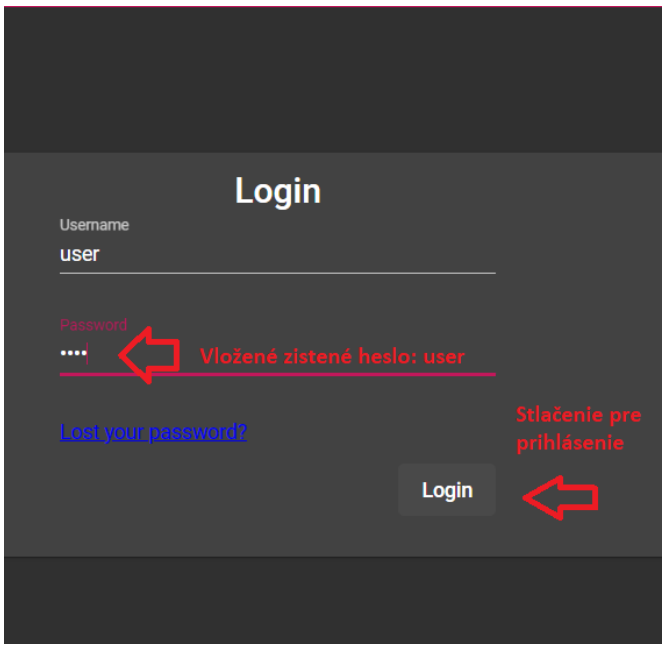
Obrázok 29: Pridanie šifrovanej podoby hesla pre druhý parameter

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.

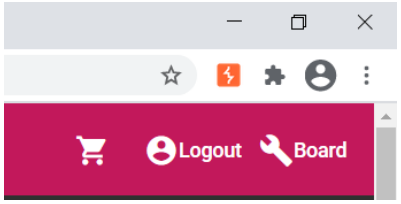


Obrázok 30: Získanie hesla pred zašifrovaním

19. 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 31: Overenie získaného hesla pre používateľa user prihlásením

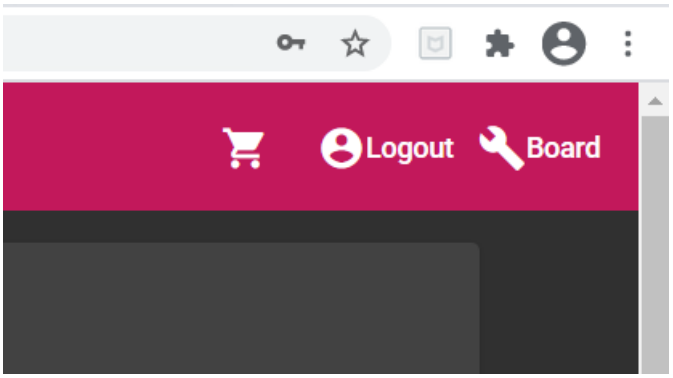


Obrázok 32: Overenie role asistenta

Použitie SQL injekcie

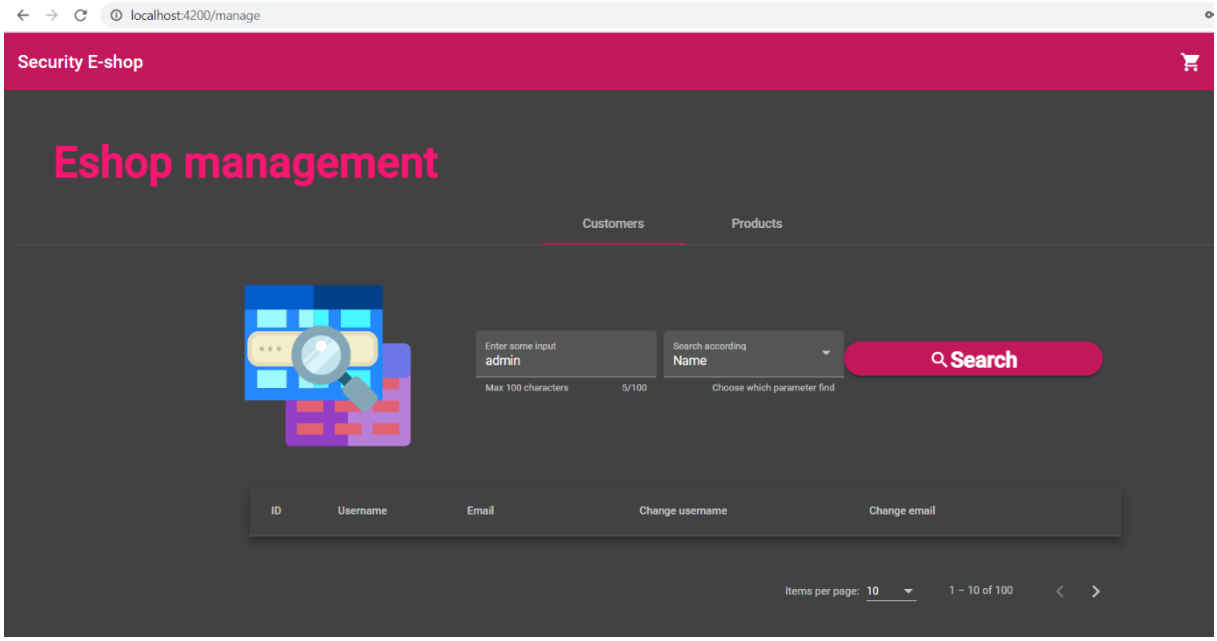
Útočník pri prelamovaní hesiel sa bol schopný dostať do role pracovníka v obchode. Následne má prístup k používateľským emailom a menám. Jeho úlohou bude ale vyhľadať admina, ktorý sa nezobrazuje. Použije SQL injekciu. V tejto časti ponúkame postup pri scenári aplikovania SQL injekcie.

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



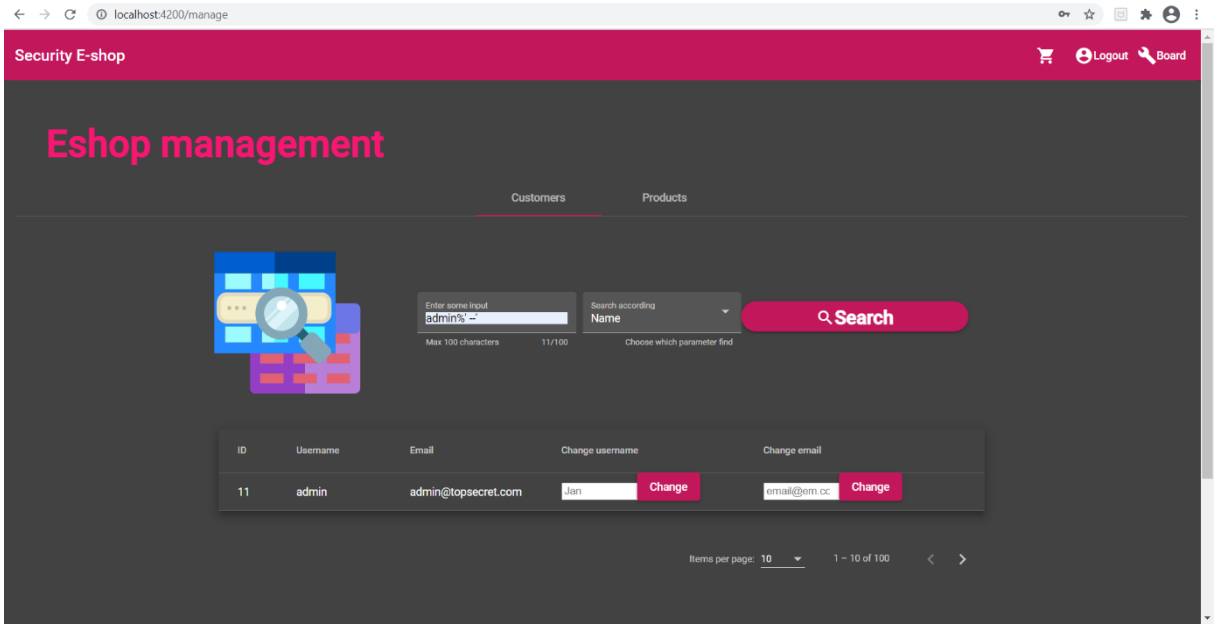
Obrázok 33: Pracovník v obchode má prístup k tabuli používateľov

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



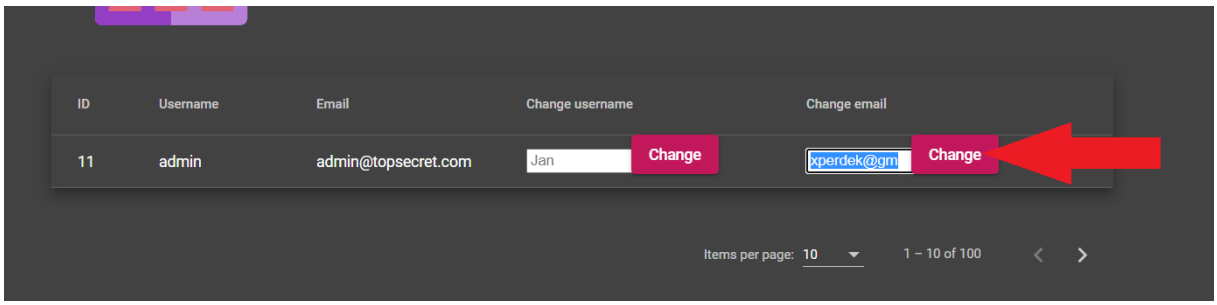
Obrázok 34: Pokus vyhľadať používateľa s menom admin

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



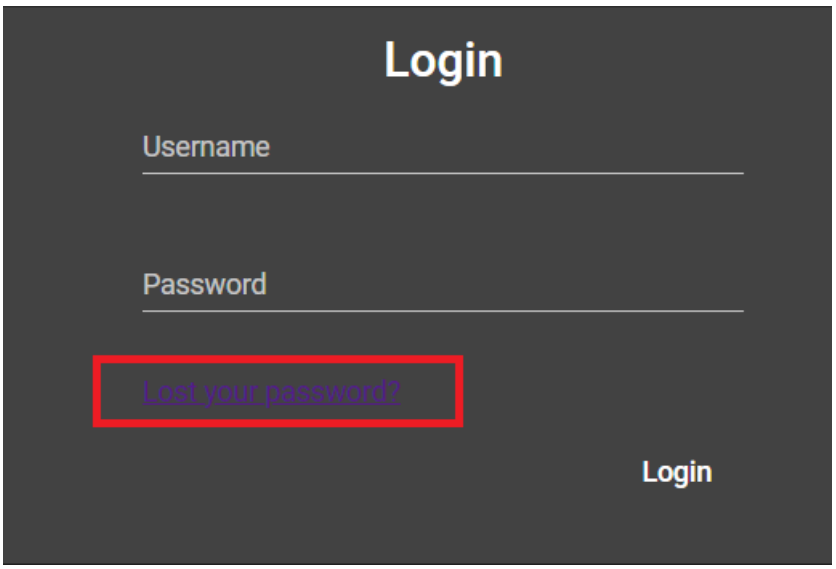
Obrázok 35: Použitie SQL Injekcie pre vyhľadanie používateľa s menom admin

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



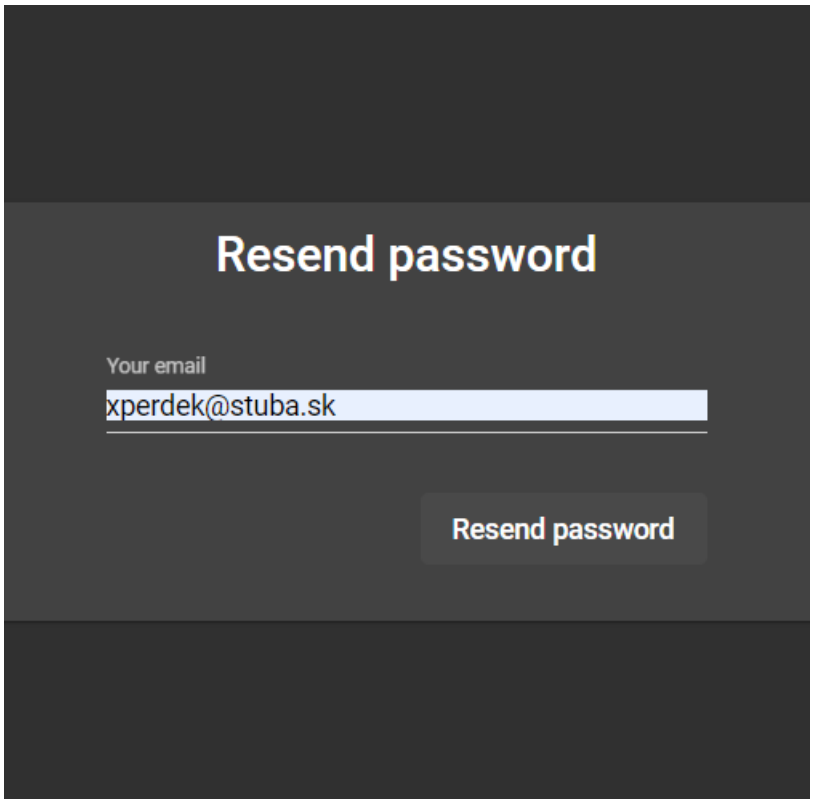
Obrázok 36: Zmena emailovej adresy používateľa admin na svoj vlastný

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



Obrázok 37: Prihlasovací formulár s odkazom na obnovu zabudnutého hesla

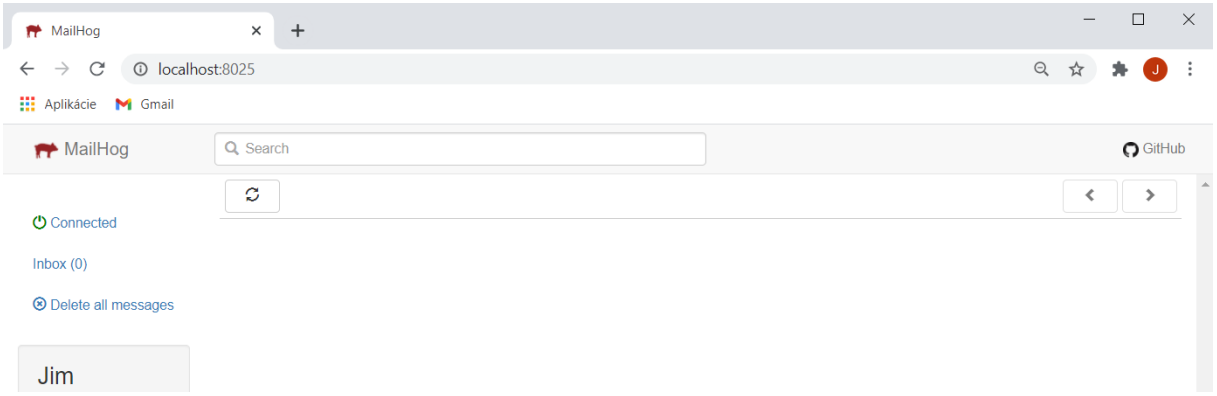
6. Na nasledujúcom formulári zadajte zmenený email a kliknite na tlačidlo Resend password.



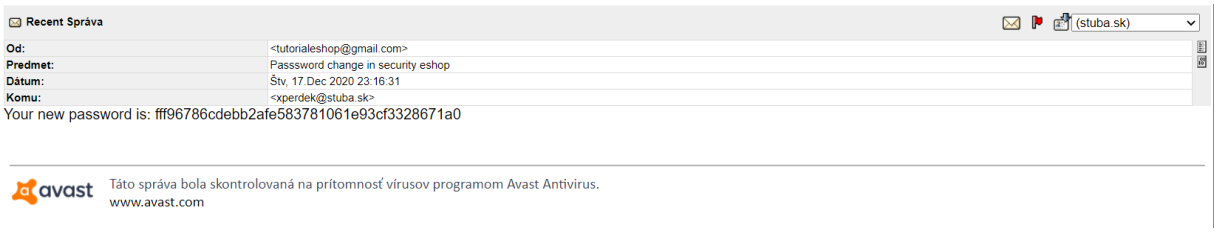
Obrázok 38: Formulár pre pregenerovanie nového hesla

7. Otvorte svojho emailového klienta a počkajte kým vám príde email z eshopu. Potom z neho získajte heslo. Ak používate aplikáciu nasadenú lokálne v prostredí docker, tak mail by mal byť doručený do MailHog aplikácie dostupnej na adrese localhost:8025 (kvôli zabezpečeniu emailového účtu nefunguje prihlásenie do mailu, keďže každý používateľ má iné zariadenie a Gmail prihlásenie zablokuje). Obsah mailu by mal byť identický ako v predchádzajúcom prípade.

Obrázok 39: Doručenie správy so zmeneným heslom

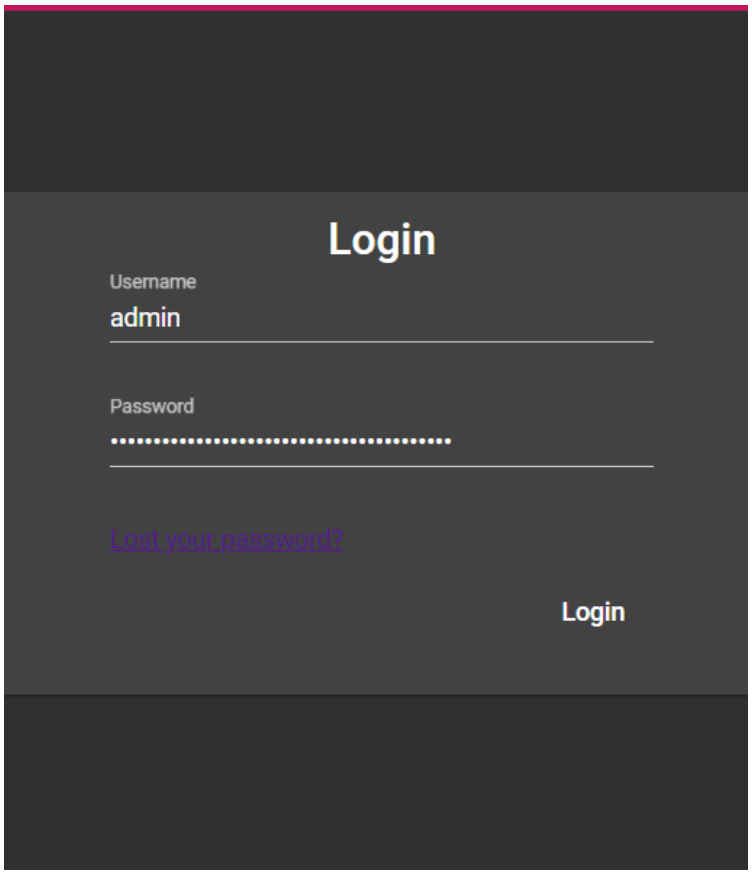


Obrázok 40: MailHog dostupný pre lokálne nasadenie



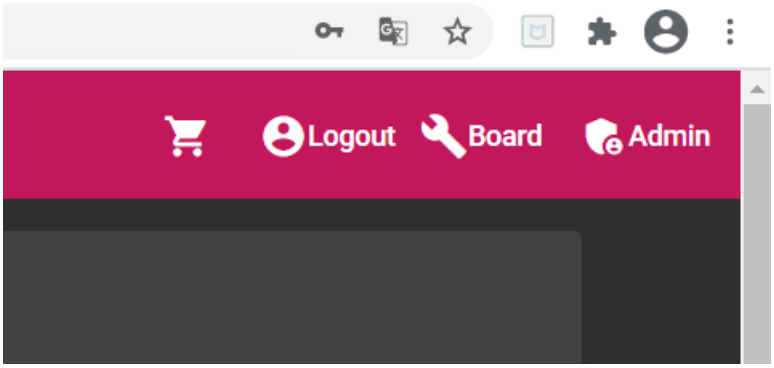
Obrázok 41: Zmenené heslo sa nachádza v správe

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

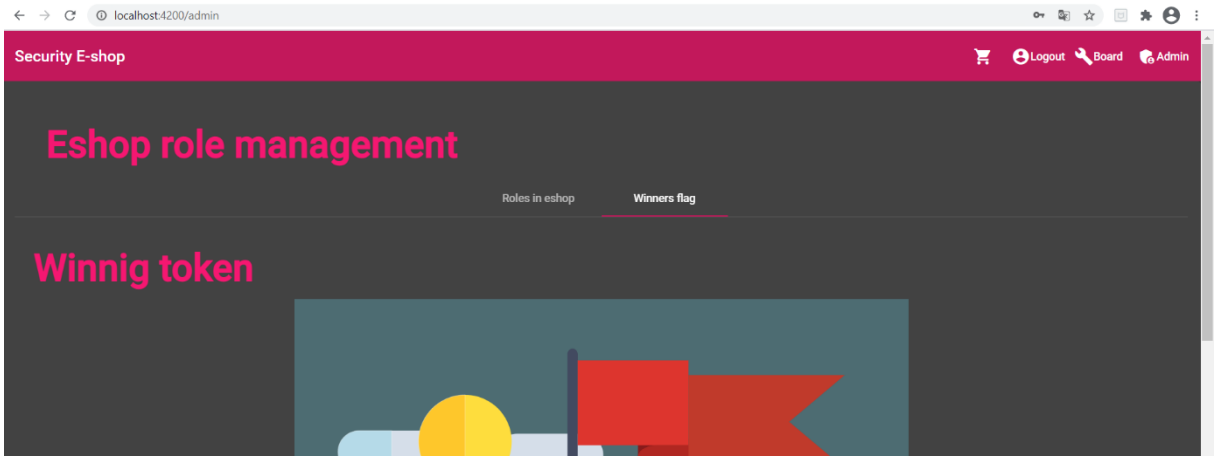


Obrázok 42: Vloženie zmenených údajov do formulára pre prihlásenie

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 43: Používateľ s privilégiom admin má vlastný ovládací panel

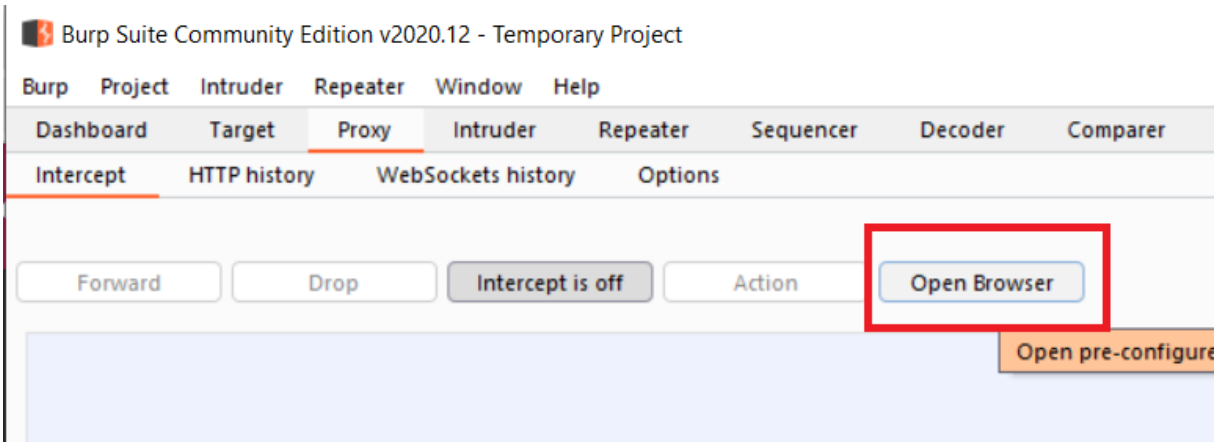


Obrázok 44: Prekliknutie sa na víťazný token

Ukradnutie produktu z eshopu

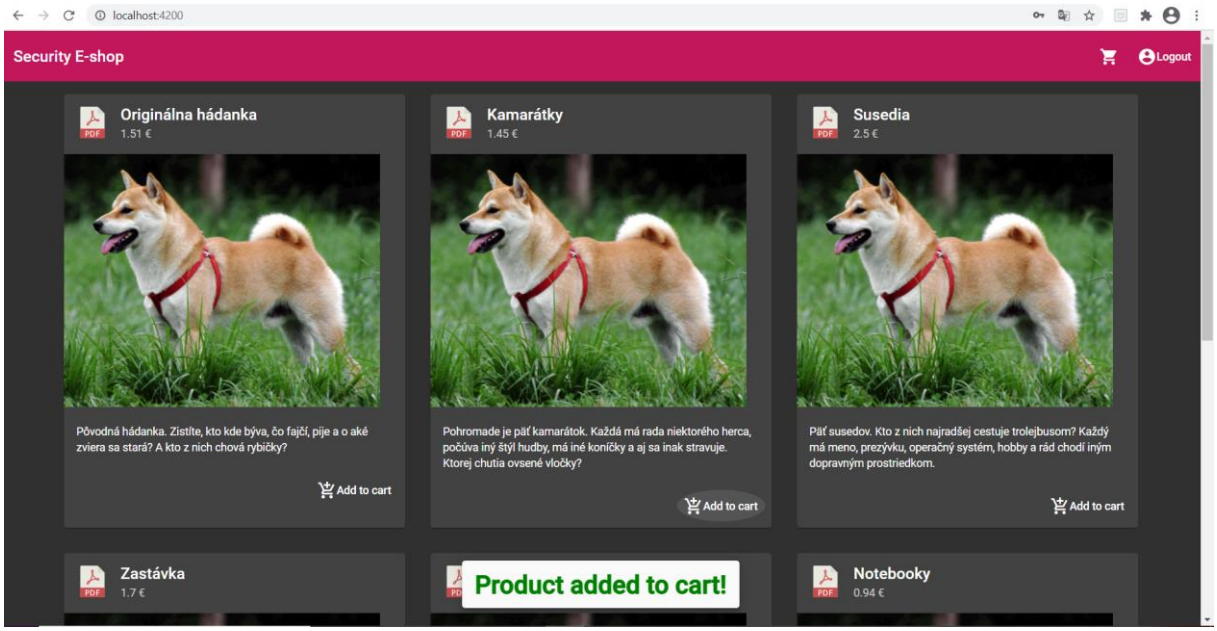
Útočník ukradne produkty z eshopu tým, že pošle vo formulári nulovú hodnotu. Najprv ale musí vytvoriť objednávku.

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



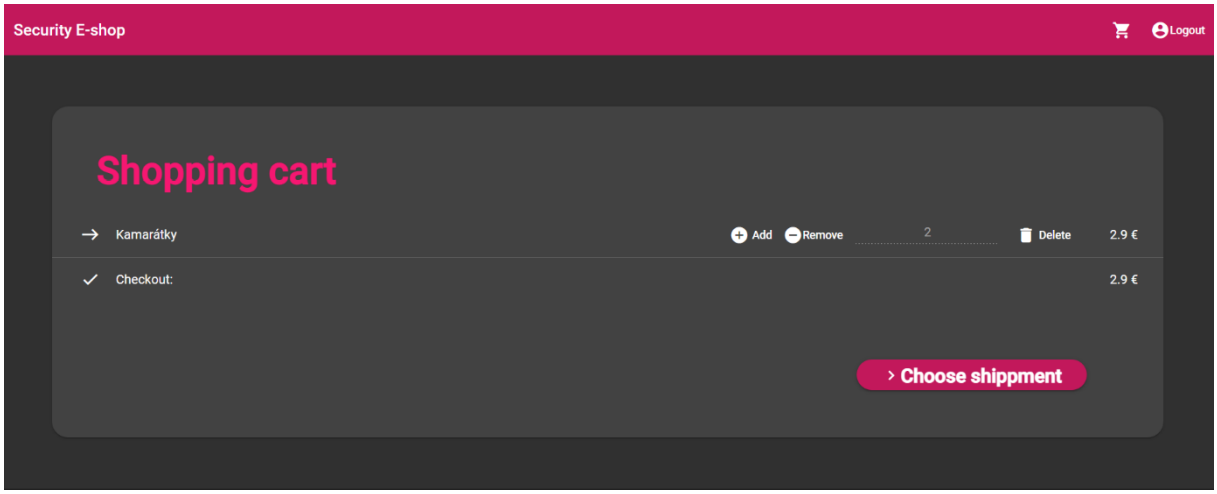
Obrázok 45: Zapnutie burpsuite a otvorenie vlastného prehliadača

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



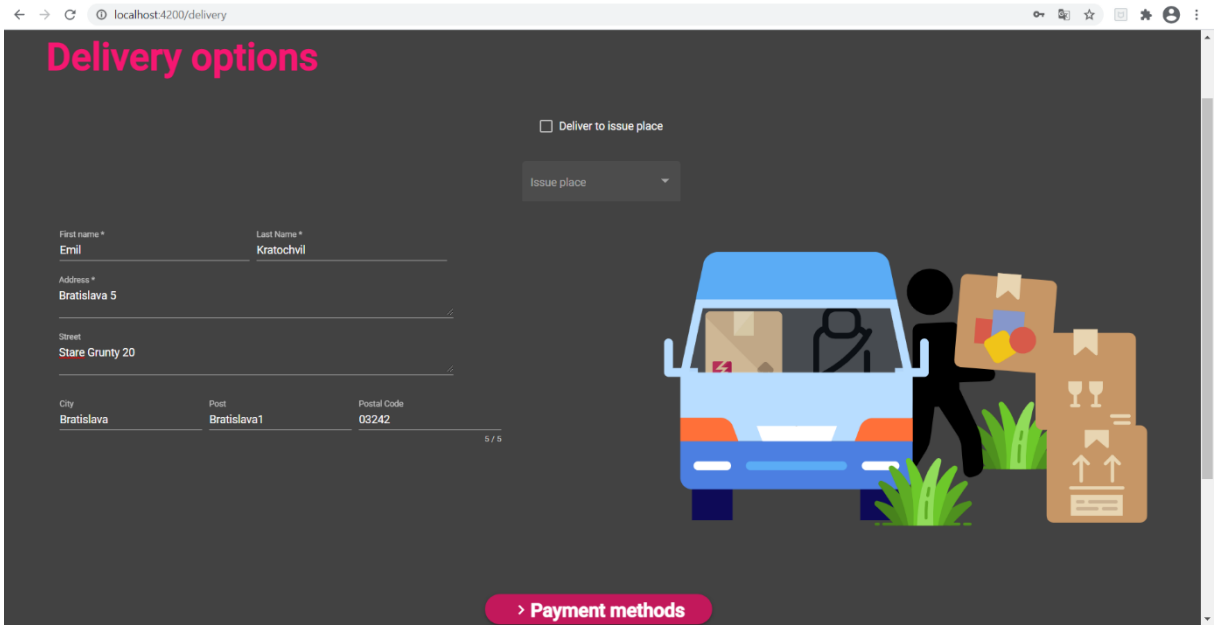
Obrázok 46: Pridanie produktu do košíka

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



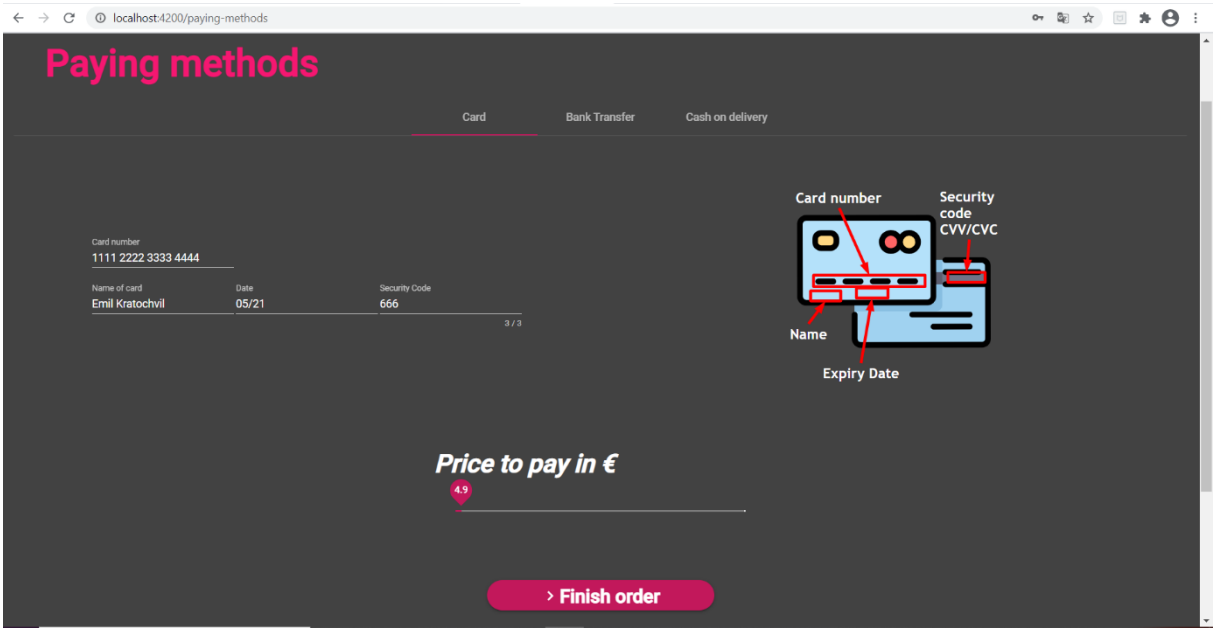
Obrázok 47: Potvrdenie produktov v košíku

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



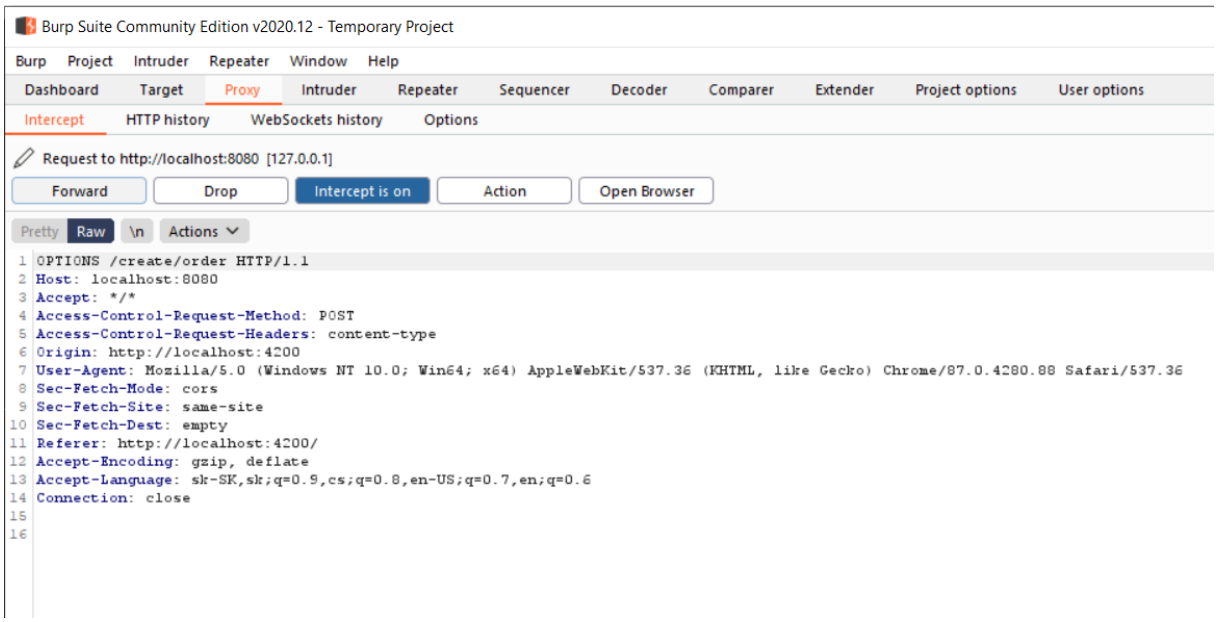
Obrázok 48: Určenie dodacej adresy

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



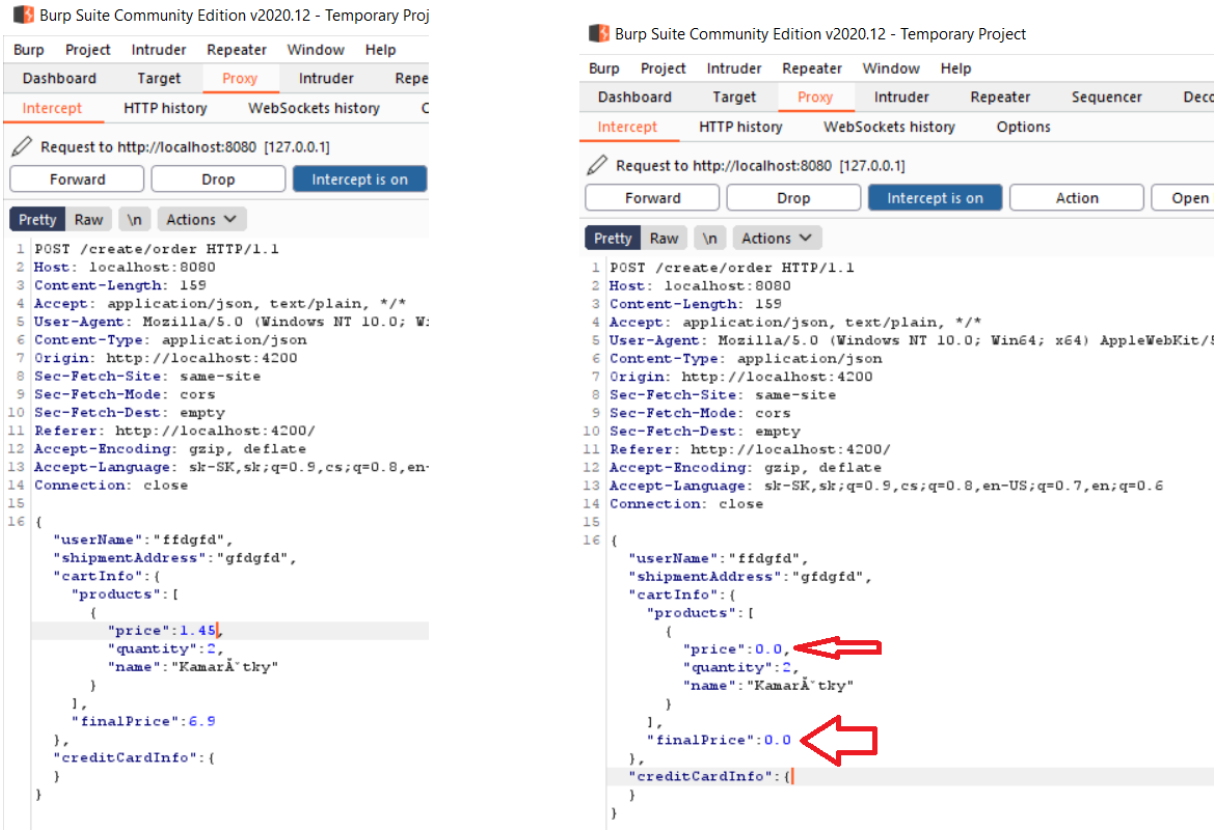
Obrázok 49: Zadanie informácií o platbe a potvrdenie

6. Prvý request prepošlite stlačením tlačidla forward.



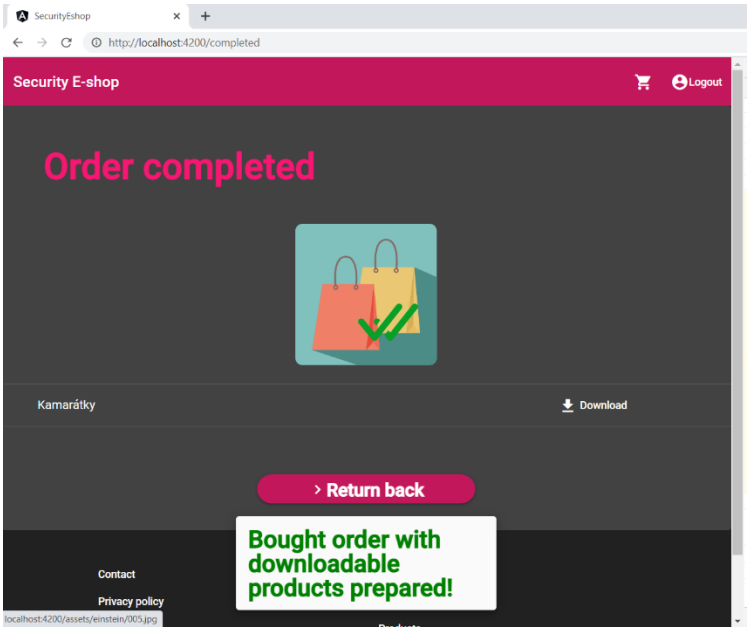
Obrázok 50: Ignorovanie prvého requestu

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



Obrázok 51: Zmena informácií v druhom requeste

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

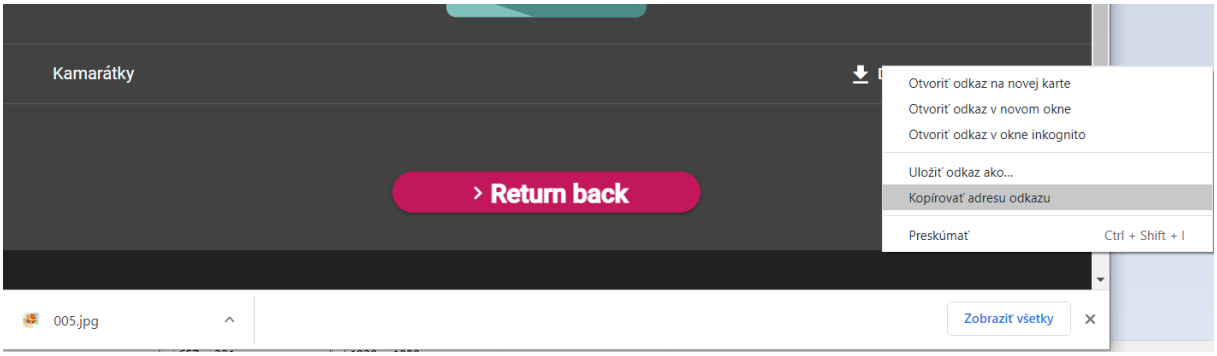


Obrázok 52: Stiahnutie ukradnutých produktov

Získanie prístupu k súborom

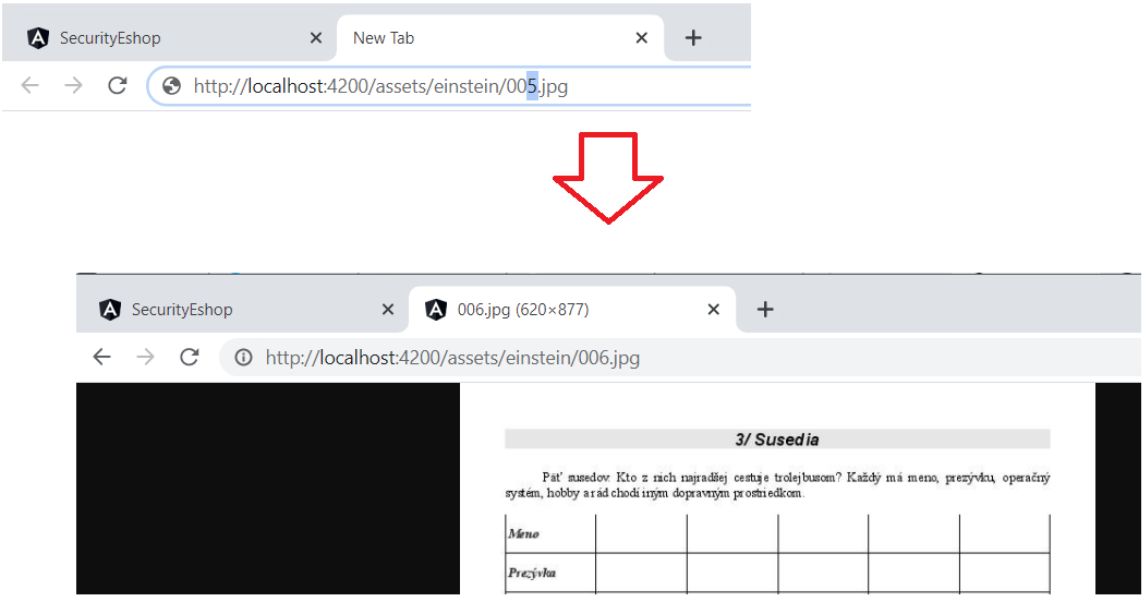
Útočník by mal vedieť, že ako technológia bol použitý Angulár. Na základe tejto informácie by mal byť schopný dostať sa k verejne uloženým súborom na stránke zadaním do prehliadača cestu k assets/images. Už je len potrebné zistiť presnú cestu. Pri minulom scenári s ukradnutím produktu si ale môže všimnúť, 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 53: Získanie odkazu na stiahnutý obsah

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



Obrázok 54: Vyskúšanie podobnej adresy s inkrementovaným číslom obrázka