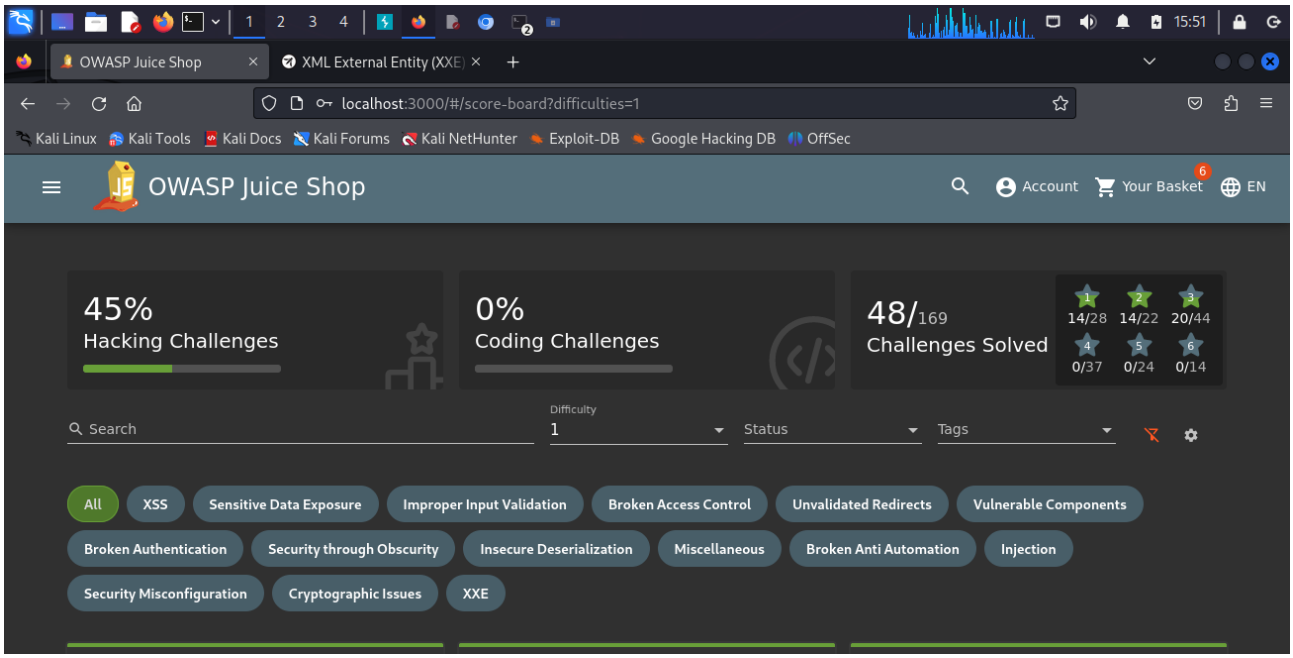
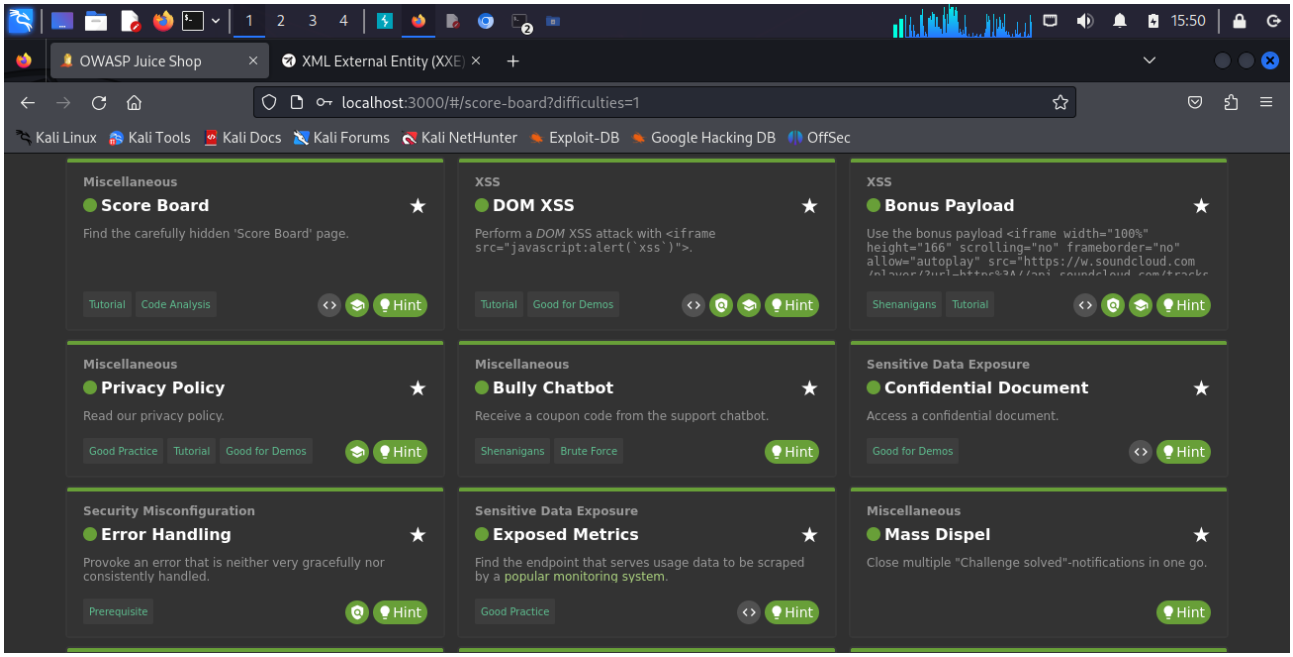
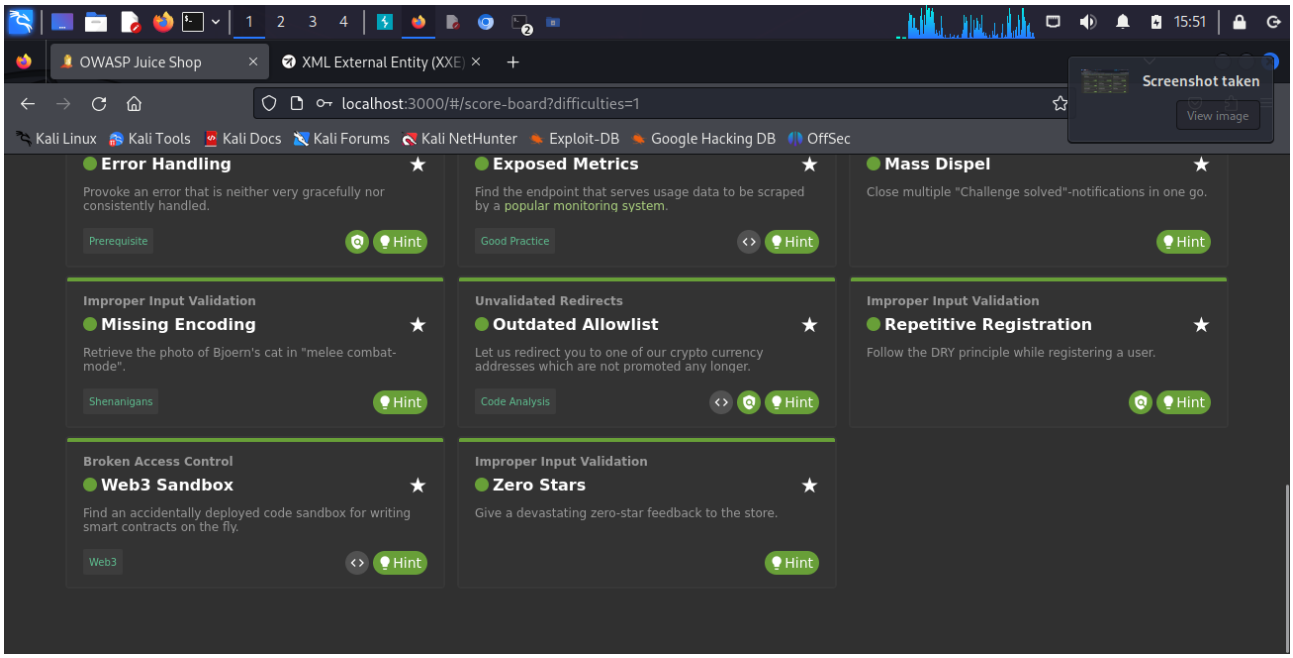


Slika 1: Ukupan broj rešenih izazova



Slika 2: Rešeni izazovi težine ★



Slika 3: Rešeni izazovi težine ★

1. ★ **Score Board**
Ranjivost: Score Board je bio vidljiv samo korisnicima s posebnim pravima pristupa. Ova ranjivost omogućava pregled svih izazova i njihov status.
Rešenje: Pristup Score Board-u ostvaren je kroz URL manipulaciju, gde je direktnim unosom odgovarajuće putanje prikazan sadržaj.

2. ★ **DOM XSS**
Ranjivost: Aplikacija je bila podložna DOM XSS napadu zbog nepravilne validacije unosa na klijentskoj strani.
Rešenje: Maliciozni JavaScript kod ubačen je kroz ranjivo polje unosa, što je omogućilo izvršavanje skripti u korisničkom pretraživaču.

3. ★ **Bonus Payload**
Ranjivost: Bonus Payload je ranjivost koja koristi specifičan ulaz za pokretanje neočekivanog ponašanja u aplikaciji.
Rešenje: Identifikovan je poseban zahtev u mrežnom saobraćaju i ubačen odgovarajući payload u zahtev.

4. ★ **Privacy Policy**
Ranjivost: Privacy Policy stranica je sadržala skriveni sadržaj dostupan kroz jednostavnu manipulaciju elementima stranice.
Rešenje: Pristup skrivenom sadržaju ostvaren je kroz razvojni alat pretraživača i promenu atributa vidljivosti.

5. ★ **Bully Chatbot**
Ranjivost: Chatbot je bio podložan zloupotrebama kroz unos specifičnih fraza koje pokreću neočekivane odgovore.

Rešenje: Unos ključnih reči identifikovao je ranjivost i omogućio generisanje odgovora potrebnog za rešavanje izazova.

6. ★ **Confidental Document**
Ranjivost: Dokument sa poverljivim informacijama bio je dostupan zbog slabe zaštite URL adrese.
Rešenje: Direktno pristupanje poznatom putanju omogućilo je preuzimanje dokumenta.

7. ★ **Error Handling**
Ranjivost: Detaljne greške prikazane korisniku mogu otkriti informacije o aplikaciji, poput strukture baze podataka.
Rešenje: Generisan je specifičan zahtev koji je prouzrokovao grešku, čime su prikazani korisni podaci za rešavanje izazova.

8. ★ **Exposed Metrics**
Ranjivost: Aplikacija je javno izložila endpoint sa podacima o performansama i internim statistikama.
Rešenje: Endpoint je pronađen kroz pretragu dostupnih URL-ova i pristupanjem su dobijene informacije.

9. ★ **Mass Dispel**
Ranjivost: Aplikacija nije pravilno ograničila masovno brisanje unosa, omogućavajući neautorizovane promene.
Rešenje: Zahtev za masovno brisanje simuliran je kroz alat za testiranje API-ja.

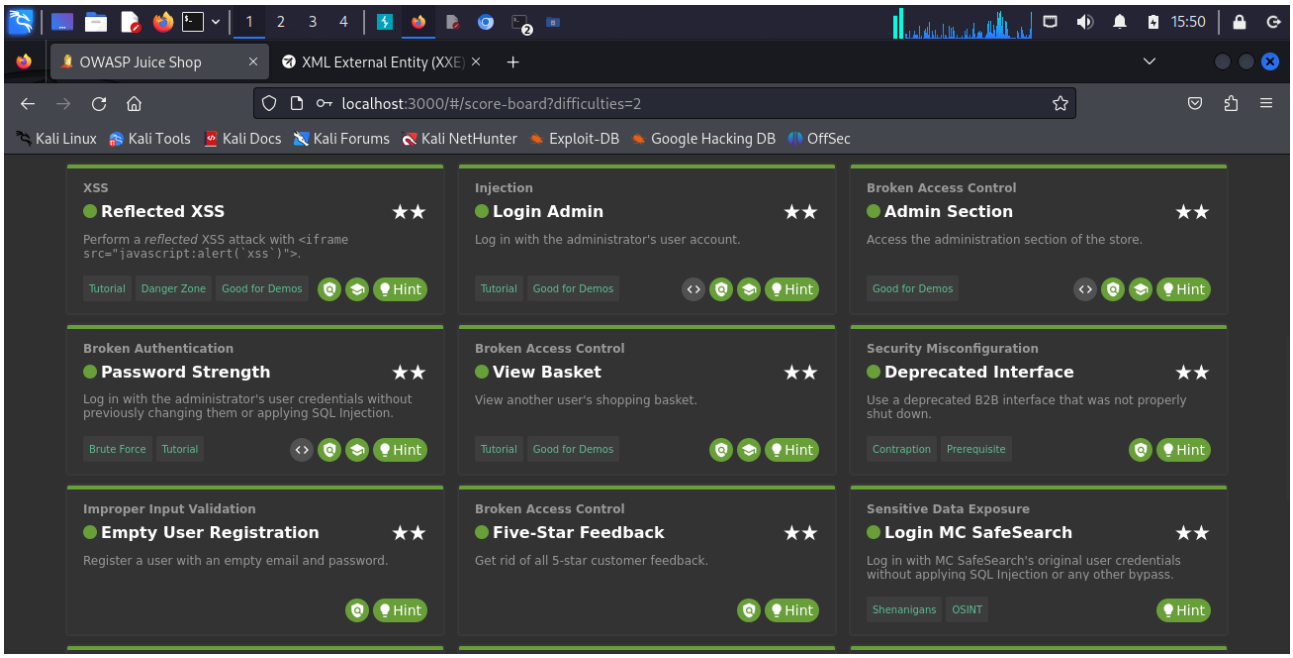
10. ★ **Missing Encoding**
Ranjivost: Nepravilna enkodacija korisničkog unosa omogućila je XSS napad kroz umetanje malicioznog sadržaja.
Rešenje: Unet je JavaScript kod u ranjivo polje, koji se izvršio na strani klijenta.

11. ★ **Outdated Allowlist**
Ranjivost: Allowlist nije ažuriran za nove domene, omogućavajući pristup neželjenim lokacijama.
Rešenje: Modifikovan je zahtev da koristi nedovoljno ograničenu vrednost, što je omogućilo prolaz.

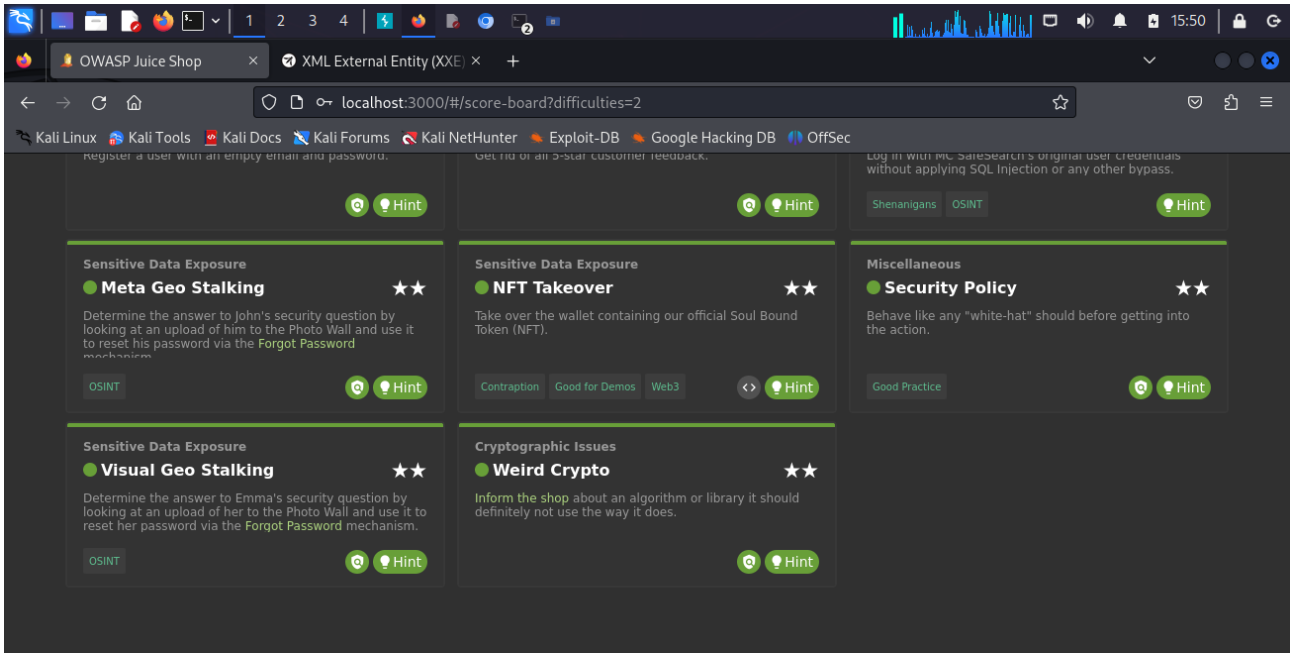
12. ★ **Repetitive Registration**
Ranjivost: Nije postojao mehanizam za sprečavanje višestrukih registracija sa istim podacima.
Rešenje: Više naloga registrovano je koristeći male varijacije unosa kako bi se testirala ranjivost.

13. ★ **Web3 Sandbox**
Ranjivost: Sandbox okruženje nije izolovalo opasne operacije, omogućavajući izvršenje štetnih radnji.
Rešenje: Kreiran je zahtev koji je zaobišao ograničenja sandbox-a i omogućio izvršenje.

14. ★ **Zero Stars**
Ranjivost: Sistem za ocenjivanje dozvoljavao je postavljanje nerealnih ocena poput nula zvezdica.
Rešenje: Manipulacijom zahtevom putem alata za mrežni saobraćaj poslata je nevalidna vrednost ocene.



Slika 4: Rešeni izazovi težine ★★



Slika 5: Rešeni izazovi težine ★★

15. ★★ **Reflected XSS**
Ranjivost: Reflektovani XSS omogućava izvršenje malicioznih skripti kroz podatke poslato serveru.
Rešenje: Unet je JavaScript kod u URL, koji se izvršio kada je server reflektovao ulaz.

16. ★★ **Login Admin**

Ranjivost: Administratorski nalog bio je ranjiv zbog slabog ili poznatog korisničkog imena i lozinke.
Rešenje: Korišćenjem brute force tehnike ili poznatih kredencijala ostvaren je pristup.

17. ★★ **Admin Section**
Ranjivost: Administratorski panel nije bio dovoljno zaštićen, omogućavajući pristup kroz direktan URL.
Rešenje: Panel je lociran istraživanjem dostupnih putanja i otvoren bez autorizacije.

18. ★★ **Password Strength**
Ranjivost: Aplikacija nije primoravala korisnike na korišćenje jakih lozinki, što je olakšalo napad.
Rešenje: Kreiran je nalog sa slabom lozinkom, čime je potvrđena ranjivost.

19. ★★ **View Basket**
Ranjivost: Korpa za kupovinu omogućavala je manipulaciju sadržajem kroz izmene u mrežnom saobraćaju.
Rešenje: Izmenjena je količina proizvoda direktno u HTTP zahtevu kako bi se testirala validacija.

20. ★★ **Deprecated Interface**
Ranjivost: Stari interfejs ostao je dostupan i omogućavao neautorizovane ili nepropisne radnje.
Rešenje: Endpoint za stari interfejs pronađen je i iskorišćen za izvršenje zadatka.

21. ★★ **Empty User Registration**
Ranjivost: Sistem za registraciju korisnika nije validirao obavezna polja, omogućavajući kreiranje praznih naloga.
Rešenje: Poslat je zahtev sa praznim vrednostima za obavezna polja, čime je nalog uspešno kreiran.

22. ★★ **Five-Star Feedback**
Ranjivost: Sistem za ocenjivanje omogućavao je slanje više petozvezdanih ocena od istog korisnika.
Rešenje: Ponavljanjem zahteva za ocenjivanje i manipulacijom podataka postignuto je više glasova.

23. ★★ **Login MC SafeSearch**
Ranjivost: Aplikacija je koristila slabo zaštićene kredencijale za nalog povezan sa MC SafeSearch funkcijom.
Rešenje: Korišćenjem poznatih kredencijala ili brute force metode ostvaren je pristup nalogu.

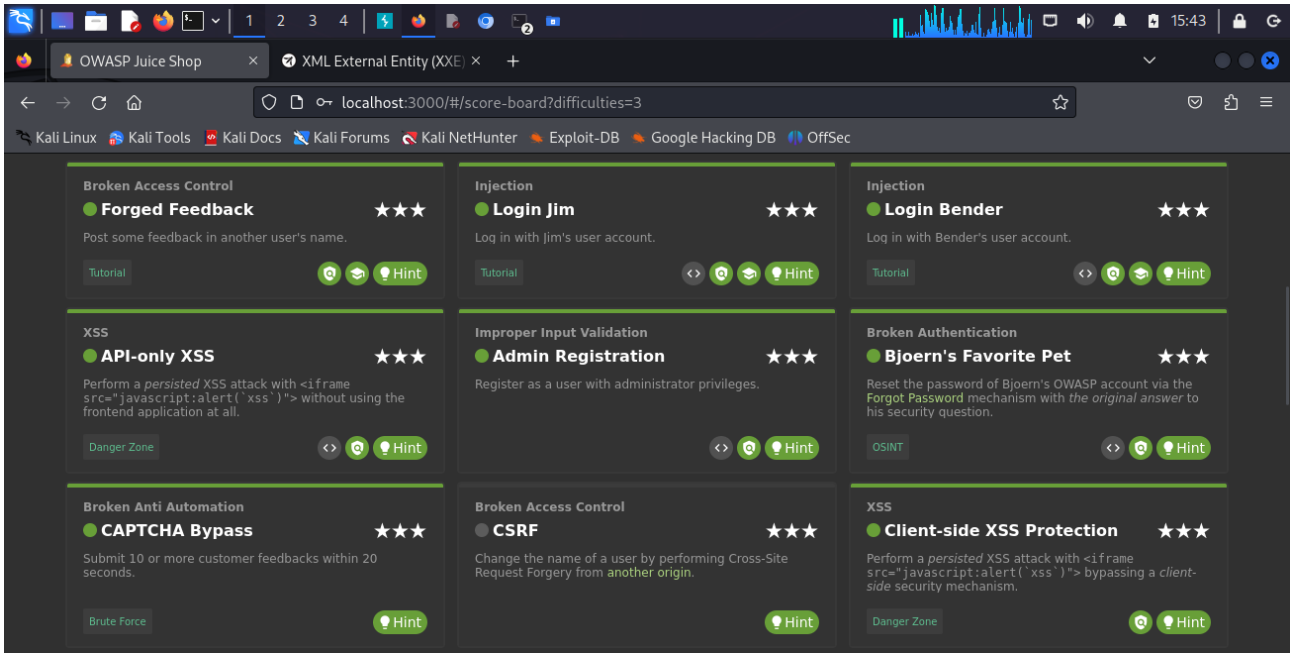
24. ★★ **Meta Geo Stalking**
Ranjivost: Meta podaci u slikama otkrivali su geolokacione informacije koje su mogle biti zloupotrebljene.
Rešenje: Analizom meta podataka iz preuzete slike locirana je potrebna informacija.

25. ★★ **NFT Takeover**
Ranjivost: NFT funkcionalnost nije pravilno proveravala vlasništvo ili autorizaciju za promene.
Rešenje: Manipulisano je zahtevom da bi se preuzela kontrola nad NFT-om.

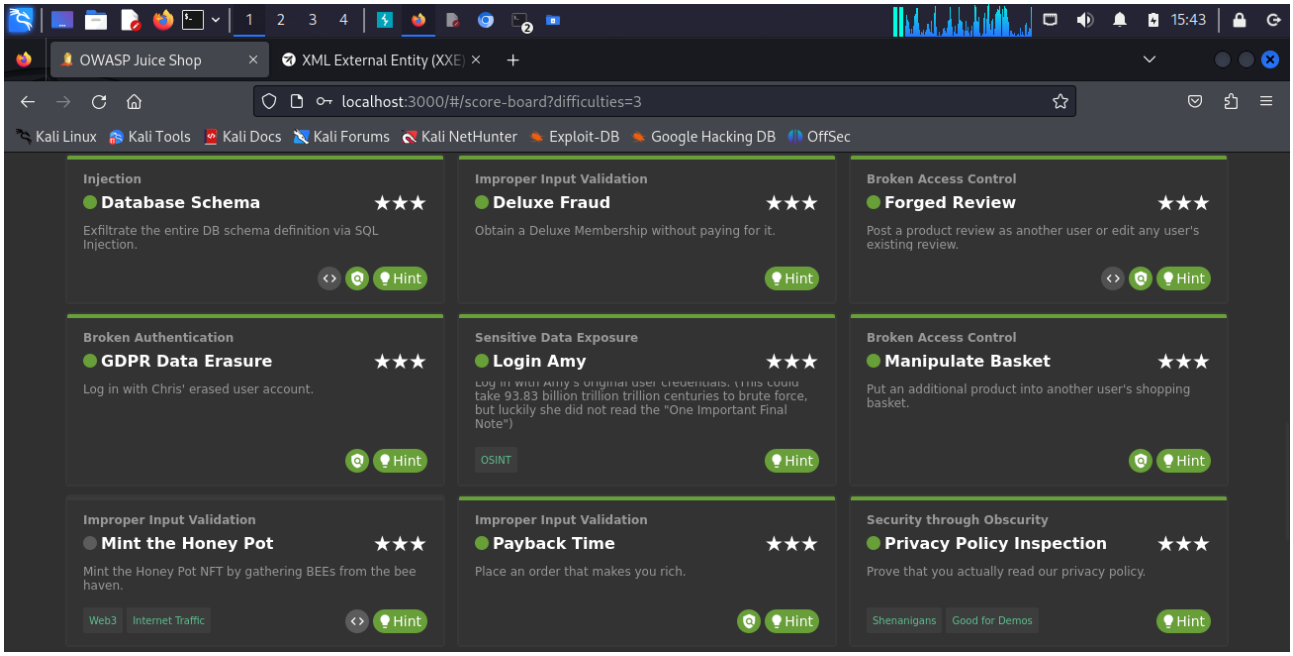
26. ★★ **Security Policy**
Ranjivost: Stranica sa politikom bezbednosti otkrivala je informacije koje mogu olakšati napad.
Rešenje: Otvorena je odgovarajuća URL putanja gde su bile dostupne skrivene informacije.

27. ★★ **Visual Geo Stalking**
Ranjivost: Geolokacija korisnika bila je ugrožena analizom vizuelnih podataka iz sadržaja aplikacije.
Rešenje: Pronađene su vizuelne informacije na slici i povezane sa stvarnom lokacijom.

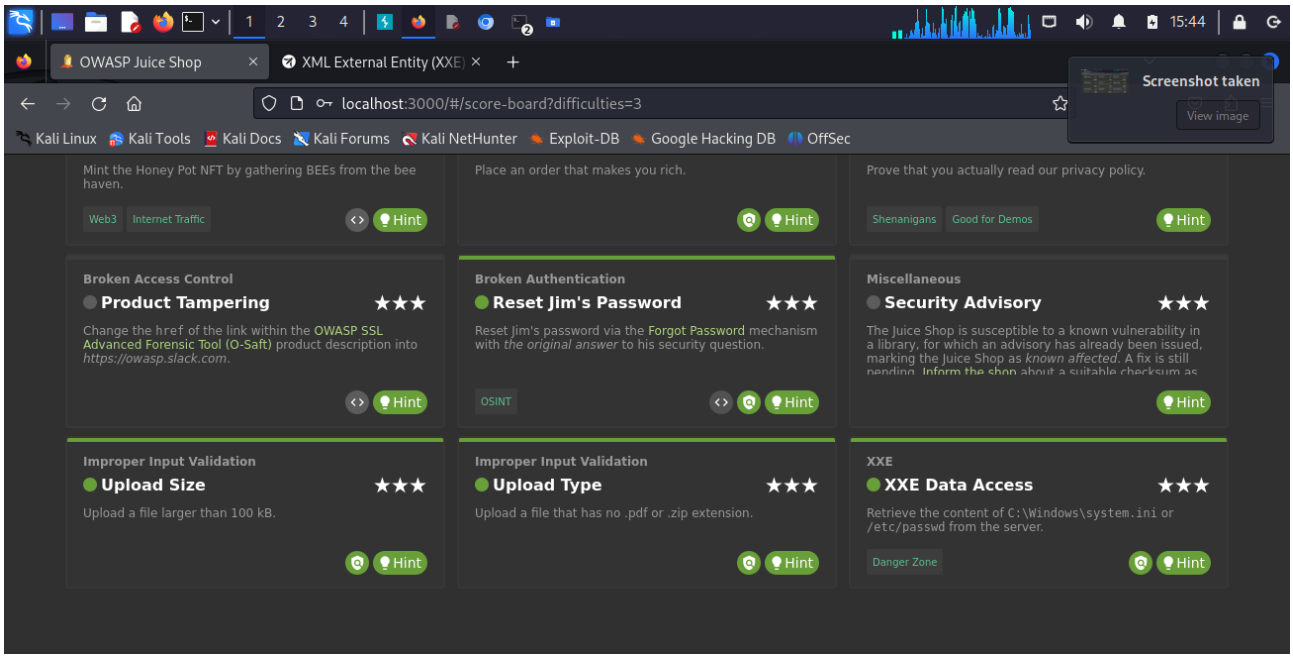
28. ★★ **Wierd Crypto**
Ranjivost: Implementacija kriptografije koristila je nesigurne ili predvidive metode za enkripciju.
Rešenje: Analizom algoritma prepoznata je slabost i generisan je validan izlaz za izazov.



Slika 6: Rešeni izazovi težine ★★★



Slika 7: Rešeni izazovi težine ★★★



Slika 8: Rešeni izazovi težine ★★★

29. ★★★ **Forget Feedback**
Ranjivost: Aplikacija nije pravilno ažurirala ili brisala stare povratne informacije korisnika.
Rešenje: Umetanjem specifičnog zahteva omogućeno je uklanjanje povratne informacije.

30. ★★★ **Login Jim**
Ranjivost: Nalog korisnika Jim bio je podložan brute force napadu zbog slabih zaštitnih mera.
Rešenje: Kombinovanjem poznatog korisničkog imena i pokušaja lozinki postignut je pristup nalogu.

31. ★★★ **Login Bender**
Ranjivost: Nalog Bendera bio je ranjiv zbog predvidivih ili lako dostupnih kredencijala.
Rešenje: Pristup je ostvaren koristeći poznate kredencijale ili manipulacijom zahteva.

32. ★★★ **API-only XSS**
Ranjivost: API endpointi omogućavali su umetanje malicioznih skripti kroz parametre bez validacije.
Rešenje: Poslat je XSS payload putem API zahteva, što je izazvalo izvršenje koda.

33. ★★★ **Admin Registration**
Ranjivost: Administratorski nalog mogao je biti kreiran zbog lošeg ograničenja u procesu registracije.
Rešenje: Manipulisana je registraciona forma da bi se dodala administratorska prava.

34. ★★★ **Bjoern‘s Favorite Pet**
Ranjivost: Skrivene informacije o omiljenom ljubimcu mogle su biti zloupotrebljene za napad.
Rešenje: Pronalaženjem tragova u aplikaciji otkriven je naziv ljubimca potreban za rešavanje.

35. ★★★ **CAPTCHA Bypass**
Ranjivost: CAPTCHA sistem nije bio dovoljno robustan i omogućavao je automatsko zaobilaženje.
Rešenje: Korišćenjem ponovljenih zahteva ili poznatog odgovora CAPTCHA je zaobiđena.

36. ☆☆☆ CSRF

37. ★★★ **Client-side XSS Protection**
Ranjivost: Klijentska validacija nije bila pravilno implementirana, što je omogućilo XSS napade.
Rešenje: Maliciozni kod ubačen je u parametre URL-a, a nedostatak zaštite omogućio je njegovo izvršavanje.

38. ★★★ **Database Schema**
Ranjivost: Otkriven je prikaz šeme baze podataka zbog nepropisne konfiguracije ili greške u aplikaciji.
Rešenje: Pregledom specifične stranice ili manipulacijom zahteva otkriveni su detalji baze podataka.

39. ★★★ **Deluxe Fraud**
Ranjivost: Sistem nije pravilno validirao promene deluxe proizvoda, omogućavajući manipulaciju cenama.
Rešenje: Izmenjeni su parametri u HTTP zahtevu kako bi se smanjila cena proizvoda.

40. ★★★ **Forget Review**
Ranjivost: Aplikacija nije pravilno rukovala zahtevima za brisanje korisničkih recenzija, omogućavajući manipulaciju.
Rešenje: Kreiran je zahtev koji je omogućio uklanjanje određene recenzije.

41. ★★★ **GDPR Data Erasure**
Ranjivost: Aplikacija nije u potpunosti implementirala GDPR brisanje podataka korisnika.
Rešenje: Simuliran je zahtev za brisanje podataka kako bi se identifikovali tragovi preostalih informacija.

42. ★★★ **Login Amy**
Ranjivost: Korisnički nalog Amy bio je ranjiv zbog slabih zaštitnih mehanizama.
Rešenje: Pristup je postignut upotrebom poznatih kredencijala ili brute force metodom.

43. ★★★ **Manipulate Basket**
Ranjivost: Korpa za kupovinu omogućavala je neovlašćene izmene u količinama i cenama proizvoda.
Rešenje: Izmenjeni su parametri u mrežnom zahtevu kako bi se simulirale promene u korpi.

44. ☆☆☆ Mint the Honey Pot

45. ★★★ **Payback Time**
Ranjivost: Sistem za refundacije nije pravilno proveravao validnost zahteva, omogućavajući zloupotrebu.
Rešenje: Generisan je zahtev za povraćaj sredstava koristeći manipulaciju podacima.

46. ★★★ **Privacy Policy Inspection**
Ranjivost: Privacy Policy stranica otkrivala je informacije koje bi mogle biti iskorišćene za napad.
Rešenje: Pregledana je stranica i identifikovane su skrivene informacije putem alata za pregled DOM-a.

47. ☆☆☆ Product Tampering

48. ★★★ **Reset Jim‘s Password**
Ranjivost: Proces za resetovanje lozinke bio je ranjiv na zloupotrebu zbog predvidivih podataka.
Rešenje: Generisan je zahtev sa poznatim informacijama o korisniku kako bi se resetovala lozinka.

49. ☆☆☆ Security Advisory

50. ★★★ **Upload Size**
Ranjivost: Ograničenje veličine za upload datoteka nije bilo pravilno implementirano, omogućavajući unos velikih datoteka.
Rešenje: Poslat je zahtev sa datotekom većom od dozvoljene veličine kako bi se testirala validacija.

51. ★★★ **Upload Type**
Ranjivost: Sistem za upload nije pravilno proveravao tip datoteke, omogućavajući upload malicioznih sadržaja.
Rešenje: Poslata je datoteka neprikladnog tipa, što je potvrdilo ranjivost.

52. ★★★ **XEE Data Access**
Ranjivost: Aplikacija je bila podložna XML External Entity (XEE) napadima, omogućavajući pristup osjetljivim podacima.
Rešenje: Modifikovan je XML payload kako bi se učitale osjetljive informacije iz servera.