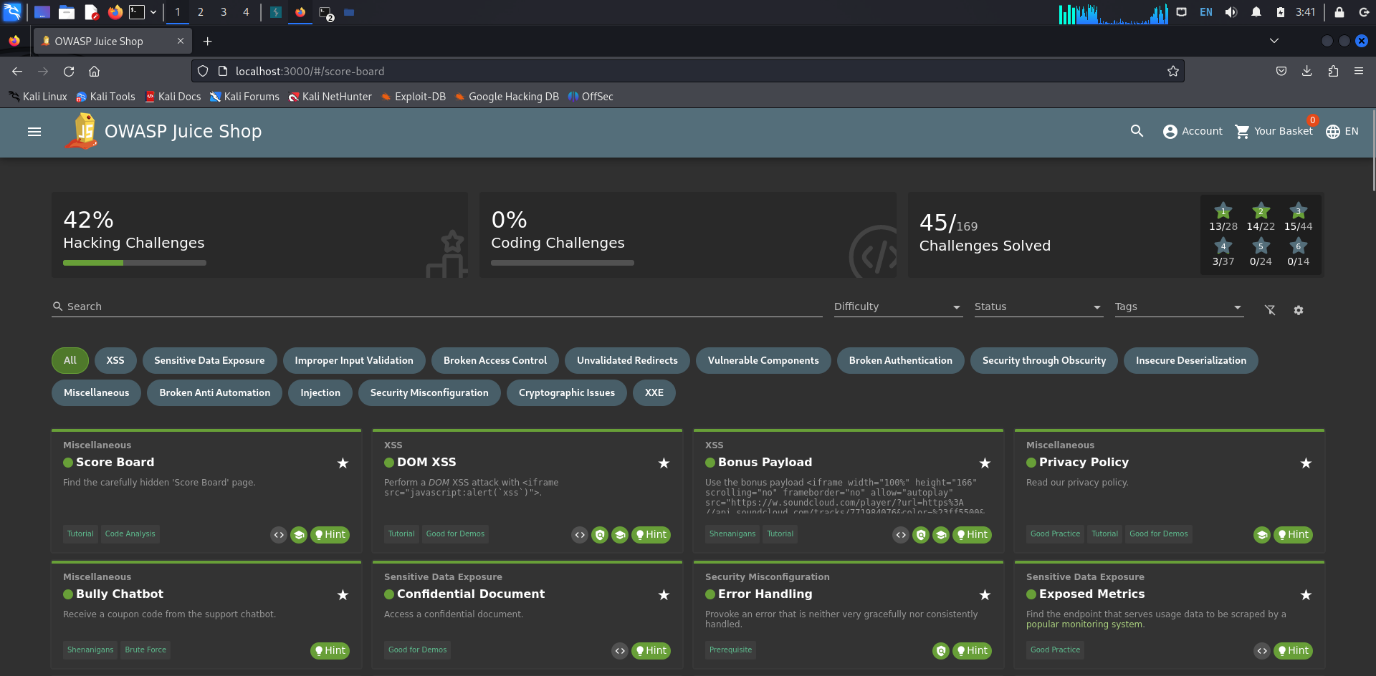
# Zaštita i oporavak softverskih sistema

# OWASP Juice Shop

## Atila Renji R2 48/2024

Ukupan broj uradjenih izazova  
  
  
  
A screenshot of a computer

Description automatically generated  
  
A screenshot of a computer

Description automatically generated  
  
A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Svi uradjeni izazovi

### Objašnjenje izazova

**1. Score Board**

Pristupio sam skrivenoj stranici *Score Board* unosom direktnog URL-a, jer nije bila dostupna u navigaciji aplikacije. Ova stranica je omogućila pregled statusa svih izazova.

**2. DOM XSS**

Izveo sam DOM-based XSS napad unošenjem malicioznog JavaScript koda u ranjivo polje koje je aplikacija prikazala bez validacije. Ovo je omogućilo izvršavanje koda na strani klijenta.

**3. Bonus Payload**

Identifikovao sam poseban zahtev aplikacije i ubacio odgovarajući payload, što je aktiviralo skriveni izazov. Payload je korišćen za pokretanje neočekivanog ponašanja aplikacije.

**4. Privacy Policy**

Pretražio sam stranicu *Privacy Policy* koristeći razvojne alate pretraživača i pronašao skrivene informacije. Ove informacije su bile nevidljive korisnicima bez tehničkog znanja.

**5. Bully Chatbot**

Simulirao sam specifične poruke chatbot-u, izazvavši reakciju koja je rezultirala dodelom kupona za popust. Ova interakcija je pokazala ranjivost sistema za podršku korisnicima.

**6. Confidential Document**

Pristupio sam poverljivom dokumentu tako što sam direktno uneo poznatu URL putanju koja nije bila javno prikazana. Dokument je sadržao osjetljive informacije koje nisu bile adekvatno zaštićene.

**7. Error Handling**

Generisao sam grešku aplikacije kroz neispravan zahtev, čime su otkrivene tehničke informacije o serveru. Ove informacije su mogle biti korisne za dalju analizu sistema.

**8. Exposed Metrics**

Otkrio sam krajnju tačku koja izlaže metrike aplikacije pretraživanjem javno dostupnih URL-ova. Ove informacije su sadržale podatke o performansama i statistici sistema.

**9. Missing Encoding**

Iskoristio sam nedostatak enkodovanja korisničkog unosa za izvršavanje JavaScript koda kroz ranjivo polje aplikacije. Ovo je omogućilo napad na korisnike koji su posećivali stranicu.

**10. Outdated Allowlist**

Uneo sam zastarele vrednosti koje su i dalje bile dozvoljene u aplikaciji zbog loše implementacije liste dozvoljenih unosa. Ovaj nedostatak je omogućio neovlašćene zahteve.

**11. Repetitive Registration**

Registrovao sam više korisničkih naloga koristeći slične podatke, jer aplikacija nije imala ograničenja za duple registracije. Ova ranjivost omogućava preopterećenje sistema.

**12. Web3 Sandbox**

Pronašao sam aktivnu razvojnu funkcionalnost za pametne ugovore koja nije bila namenjena krajnjim korisnicima. Ova opcija je trebalo da bude uklonjena tokom proizvodnje.

**13. Zero Stars**

Uneo sam ocenu od nula zvezdica manipulacijom API zahteva za ocenjivanje proizvoda. Sistem nije imao ograničenje koje bi sprečilo unose ispod minimalne vrednosti.

**14. Reflected XSS**

Ubacio sam JavaScript kod kroz URL parametar, koji je aplikacija reflektovala bez validacije, omogućavajući izvršavanje koda. Ovo je omogućilo potencijalne napade na korisnike.

**15. Login Admin**

Prijavio sam se na administratorski nalog koristeći poznate ili lako pogađane kredencijale. Sistem nije imao zaštitu od brute-force napada.

**16. Admin Section**

Pristupio sam administrativnom delu aplikacije unosom direktnog URL-a koji nije bio javno dostupan. Aplikacija nije imala odgovarajuću autentifikaciju za pristup ovom delu.

**17. Password Strength**

Napravio sam nalog koristeći veoma slabu lozinku, jer aplikacija nije imala ograničenja za složenost lozinki. Ova ranjivost povećava rizik od kompromitovanja naloga.

**18. View Basket**

Pristupio sam korpi drugog korisnika promenom ID parametra korpe u HTTP zahtevu. Ova ranjivost omogućava neovlašćen pristup korisničkim podacima.

**19. Deprecated Interface**

Pristupio sam staroj funkcionalnosti aplikacije koja nije bila isključena nakon ažuriranja sistema. Ova funkcionalnost je omogućavala korišćenje zastarelih opcija.

**20. Empty User Registration**

Registrovao sam nalog bez unošenja podataka u obavezna polja, koristeći direktnu manipulaciju HTTP zahteva. Sistem nije proveravao da li su polja pravilno popunjena.

**21. Five-Star Feedback**

Uneo sam povratne informacije s ocenom pet zvezdica menjajući podatke u API zahtevu. Ova manipulacija omogućava lažne pozitivne recenzije proizvoda.

**22. Login MC SafeSearch**

Prijavio sam se na nalog MC SafeSearch koristeći poznate kredencijale dostupne kroz ranjivost aplikacije. Sistem nije imao zaštitu od automatskog otkrivanja lozinki.

**23. Meta Geo Stalking**

Otkrio sam geografske podatke korisnika analizom metapodataka iz slika objavljenih u aplikaciji. Metapodaci nisu bili uklonjeni pre objavljivanja.

**24. NFT Takeover**

Manipulisao sam zahtevom aplikacije kako bih preuzeo kontrolu nad NFT resursima bez odgovarajuće autorizacije. Ova ranjivost omogućava neovlašćene promene podataka.

**25. Security Policy**

Pregledao sam stranicu s bezbednosnom politikom koristeći alate pretraživača i pronašao skrivene informacije. Ove informacije su mogle olakšati dalji napad.

**26. Visual Geo Stalking**

Identifikovao sam geografske lokacije korisnika koristeći slike objavljene u aplikaciji i vizuelne tragove. Slike su otkrivale više nego što je očekivano.

**27. Weird Crypto**

Otkrio sam slabost u implementaciji kriptografskih algoritama analizom koda aplikacije. Loša primena kriptografije omogućila je probijanje zaštite.

**28. Forged Feedback**

Uneo sam lažne povratne informacije koristeći manipulaciju API zahteva i podataka korisnika. Ovo omogućava izmenu recenzija bez autorizacije.

**29. Login Jim**

Prijavio sam se na nalog korisnika Jim koristeći javno dostupne kredencijale ili lako pogađane lozinke. Sistem nije imao zaštitu od pokušaja prijave više puta.

**30. Login Bender**

Slično kao kod naloga Jim, pristupio sam nalogu korisnika Bender koristeći poznate podatke za prijavu. Ova ranjivost ukazuje na loše upravljanje korisničkim nalozima.

**31. Admin Registration**

Kreirao sam administratorski nalog manipulišući registracionim zahtevima poslatim serveru. Sistem nije proveravao status korisnika tokom procesa registracije.

**32. Bjoern's Favorite Pet**

Otkrio sam ime ljubimca korisnika Bjoern istraživanjem tragova ostavljenih u aplikaciji. Informacija je bila sakrivena, ali dostupna pažljivom analizom sadržaja aplikacije.

**33. CAPTCHA Bypass**

Automatizovao sam unos podataka i zaobišao CAPTCHA mehanizam koristeći skriptu. Aplikacija nije imala ograničenja za broj poslatih zahteva.

**34. Deluxe Fraud**

Manipulisao sam zahtevima za kupovinu kako bih dobio *Deluxe* članstvo bez plaćanja. Sistem nije validirao podatke poslate preko API-ja.

**35. Forged Review**

Uneo sam lažnu recenziju proizvoda koristeći manipulaciju API zahteva, predstavljajući se kao drugi korisnik. Sistem nije proveravao autentičnost autora recenzije.

**36. GDPR Data Erasure**

Simulirao sam zahtev za brisanje korisničkih podataka prema GDPR pravilima i proverio da li su informacije zaista uklonjene. Sistem je zadržavao određene podatke uprkos zahtevima.

**37. Login Amy**

Prijavio sam se na nalog korisnice Amy koristeći lako pogađane kredencijale. Loša politika lozinki omogućila je pristup nalogu bez složene šifre.

**38. Manipulate Basket**

Izmenio sam sadržaj korpe drugog korisnika menjajući parametre u API zahtevima. Sistem nije validirao ID korisnika prilikom pristupa korpi.

**39. Payback Time**

Generisao sam zahtev za povraćaj sredstava koristeći manipulaciju podacima u API zahtevu. Sistem nije proveravao validnost zahteva za povraćaj novca.

**40. Privacy Policy Inspection**

Pregledao sam skrivene informacije na stranici *Privacy Policy* koristeći razvojne alate pretraživača. Informacije su bile nevidljive običnim korisnicima.

**41. Reset Jim's Password**

Resetovao sam Jimovu lozinku odgovaranjem na predvidljivo sigurnosno pitanje. Sistem nije imao odgovarajuću validaciju odgovora.

**42. Upload Type**

Uploadao sam datoteku nepravilnog tipa menjajući ekstenziju fajla tokom slanja zahteva. Sistem je proveravao samo ekstenziju, a ne i stvarni sadržaj fajla.

**43. Access Log**

Pristupio sam server logovima identifikovanjem poznatih URL-ova i direktorijuma. Ovi logovi su otkrivali osjetljive podatke o korisnicima i aplikaciji.

**44. Christmas Special**

Pronašao sam specifičnu božićnu ponudu pretragom poznatih putanja aplikacije. Sistem je zadržao staru promociju koja nije bila javno dostupna, ali je i dalje funkcionisala.