Este Black Friday. Mii de oameni cumpără frenetic. În spatele site-ului vostru de eCommerce, un singur *request* injectat cu o linie de cod SQL șterge baza de date cu comenzile.

Sau un link aparent inofensiv - trimis printr-un email de “promoție” - fură cookie-urile clienților voștri, permițând unui atacator să cumpere pe banii lor.

Sau poate un simplu formular de login, implementat în grabă, permite unui necunoscut să devină administratorul magazinului.

Asta e realitatea în care trăim.

În eCommerce, un mic punct vulnerabil poate însemna pierderi de zeci sau sute de mii de euro, procese legale, distrugerea reputației și, cel mai grav, pierderea încrederii clienților.

British Airways (2018) – Magecart Attack

- Hackerii au injectat un script de Card Skimming (XSS combinat cu interceptare de formular) direct în pagina de plată.
- Timp de 15 zile, toate datele cardurilor introduse de clienți au fost trimise către serverele atacatorilor.
- 380.000 de carduri compromise.
- British Airways a primit o amendă record de 183 de milioane de lire sterline.

British Airways faces record £183m fine for data breach

8 July 2019

Share Save

Heartland Payment Systems (2008) – SQL Injection

- Un atac prin SQL Injection a expus peste 130 de milioane de carduri de credit.
- Hackerii au folosit o vulnerabilitate banală într-un script de validare a utilizatorilor.
- Considerat unul dintre cele mai mari breșe de date din istorie.

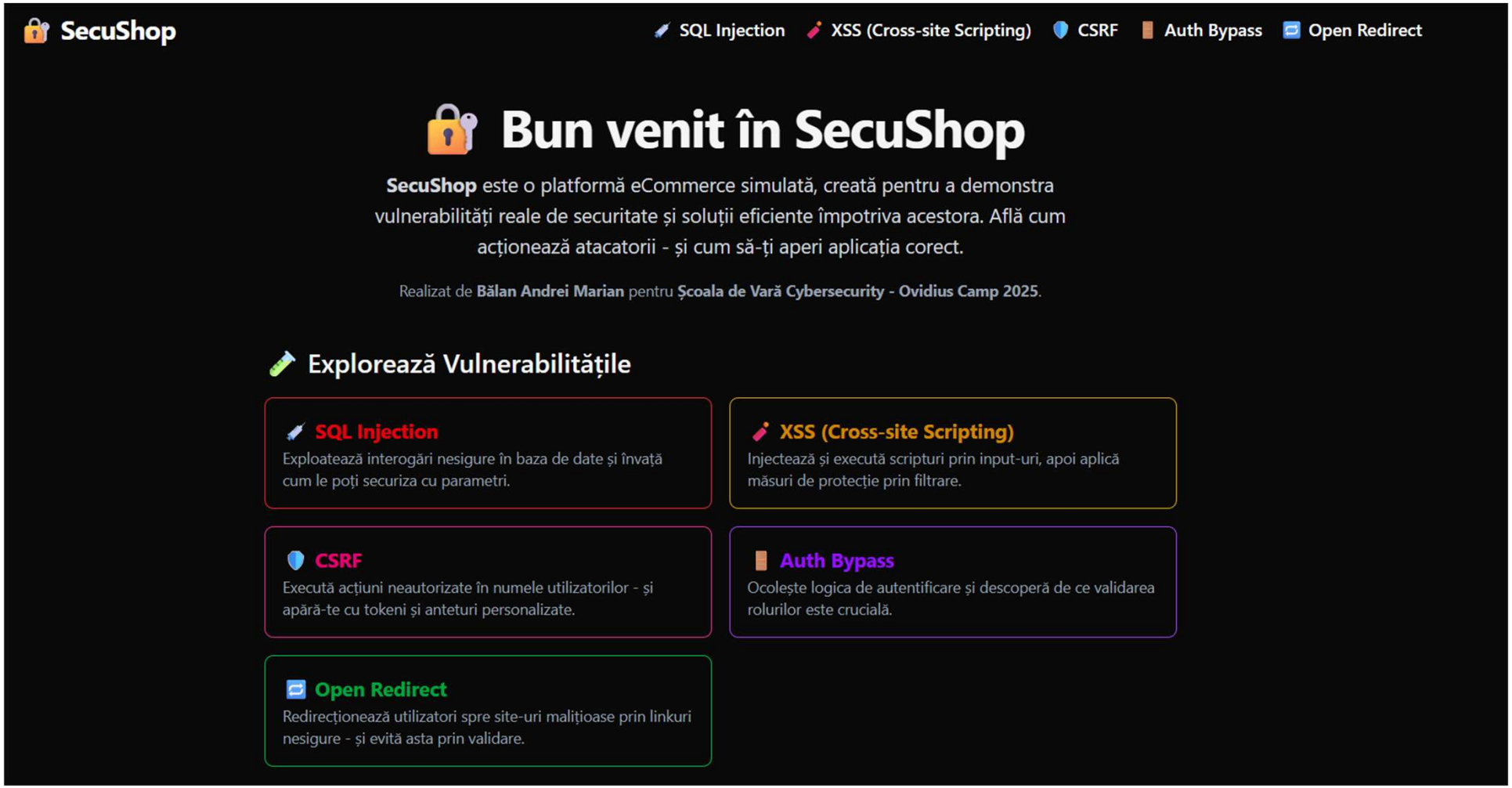
Tesco Bank (2016) – Auth Bypass și Open Redirect

- Un atac combinat: Auth Bypass + Open Redirect.
- Hackerii au reușit să fure 2.5 milioane de lire din conturile clienților.
- Au folosit un redirect malițios și tokenuri nesigure.

FCA fines Tesco Bank £16.4m for failures in 2016 cyber attack

Press Releases | First published: 01/10/2018 | Last updated: 01/10/2018

Proiectul pe GitHub


SecuShop
SQL Injection
XSS (Cross-site Scripting)
CSRF
Auth Bypass
Open Redirect
Bun venit în SecuShop
SecuShop este o platformă eCommerce simulată, creată pentru a demonstra vulnerabilități reale de securitate și soluții eficiente împotriva acestora. Află cum acționează atacatorii - și cum să-ți aperi aplicația corect.
Realizat de Bălan Andrei Marian pentru Școala de Vară Cybersecurity - Ovidius Camp 2025.
Explorează Vulnerabilitățile
SQL Injection
Exploatează interogări nesigure în baza de date și învață cum le poți securiza cu parametri.
XSS (Cross-site Scripting)
Injectează și execută scripturi prin input-uri, apoi aplică măsuri de protecție prin filtrare.
CSRF
Execută acțiuni neautorizate în numele utilizatorilor - și apără-te cu tokeni și anteturi personalizate.
Auth Bypass
Ocolește logica de autentificare și descoperă de ce validarea rolurilor este crucială.
Open Redirect
Redirecționează utilizatori spre site-uri malițioase prin linkuri nesigure - și evită asta prin validare.

Inputul este inserat direct în query. Poți testa exploatarea.

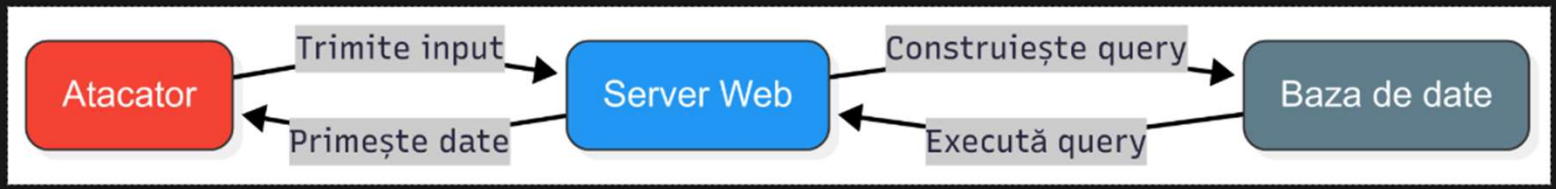
Interogare parametrizată care previne injectarea.

🧠 Cum funcționează SQL Injection?

- Atacatorul introduce text malițios în formularul de căutare.
- Serverul inserează direct acest text în query-ul SQL.
- Baza de date interpretează comanda, permițând vizualizarea sau modificarea datelor.

📊 Fluxul unui atac SQL Injection

Diagrama de mai jos arată cum inputul nefiltrat compromite baza de date:



Găsește cele mai bune produse la prețuri avantajoase.

Categorii

Electronice
Haine
Cărți
Jucării

Cele mai vândute

- Căști Wireless
- Hanorac SecuShop
- Joc de societate

⚠ **Vulnerabilitate activă!** Această căutare folosește query-uri nesecurizate.

Caută produse

`' OR 1=1 --` `' UNION SELECT id, email, password FROM User --` `' UNION SELECT null, sqlite_version(), null --`

' UNION SELECT id, email, password FROM User --

Caută

⚠ Posibilă tentativă de SQL Injection detectată!

Rezultate produse

Laptop
2500 RON

admin@example.com
admin123 RON

Masina
20000 RON

SecuShop Secure

Produse Oferte Contact

0 produse în

Căutare Protejată cu Interogări Parametrizate

Această pagină previne SQL Injection folosind interogări sigure.

Categorii

Electronice

Haine

Cărți

Jucării

Cele mai vândute

- Căști Wireless
- Hanorac SecuShop
- Joc de societate

Protejat Această căutare folosește interogări parametrizate. Codul SQL malițios este blocat automat.

Caută produse în siguranță

laptop

Caută

Rezultate produse

🧨 XSS (Cross-Site Scripting)

XSS este o vulnerabilitate critică ce permite rularea de cod JavaScript injectat de atacatori în paginile web vizitate de alți utilizatori. În continuare, vei vedea cum funcționează și cum o poți preveni.

⚠ Varianta vulnerabilă

Codul NU filtrează inputul. Comentariile sunt inserate direct în DOM.

Varianta protejată

Codul curăță datele cu `sanitize-html` pentru a preveni XSS.

🔍 Cum apare vulnerabilitatea?

Când inputul utilizatorului este inserat în DOM fără nicio filtrare, orice tag HTML sau script este executat în browser:

```
<div dangerouslySetInnerHTML={{ __html: userComment }} />
```

Orice comentariu care conține `<script>` va rula automat în browserul altor vizitatori.

🛡️ Cum prevenim atacul?

Categorii populare

Electronice

Gaming

Îmbrăcăminte

Accesorii

Promoții speciale

🎁 Transport gratuit la comenzile peste 200 RON!

⚠️ **Avertisment XSS activ!** Comentariile sunt afișate fără filtrare. Inserarea de cod JavaScript este posibilă.

Mouse Gamer RGB Bestseller

★★★★★ (124 recenzii)

Mouse performant cu iluminare RGB și DPI ajustabil.

149 RON

Adaugă în coș

Scrie o recenzie (XSS Vulnerabil)

Autor

Ex: Ana

Comentariu

Ex: <script>alert('XSS')</script>

tul meu

fil

ric comenzi

tofel

ări

Avertisment: Backend-ul acceptă cereri POST fără validare. Acest lucru permite transferuri neautorizate (CSRF).

💰 Sold curent: 500 RON

🚨 Trimite 100 RON

📜 Istoric tranzacții

Niciun transfer efectuat în această sesiune.

🔓 Simulare atac CSRF real

Un site malițios poate include un iframe ascuns care trimite cereri POST fără acordul tău.

Pretty-print ☐


```
{"message":"Transfer reușit. Sold rămas: 500 RON"}
```


Această iframe simulează un atac real. Dacă vezi tranzacții noi în istoric, exploit-ul a funcționat.

Contul meu

- Profil
- Istoric comenzi
- Portofel
- Setări

✅ Cererile POST necesită tokenul CSRF unic generat per sesiune.

💰 **Sold curent:** 500 RON

🔒 Trimite 100 RON

📜 **Istoric tranzacții**

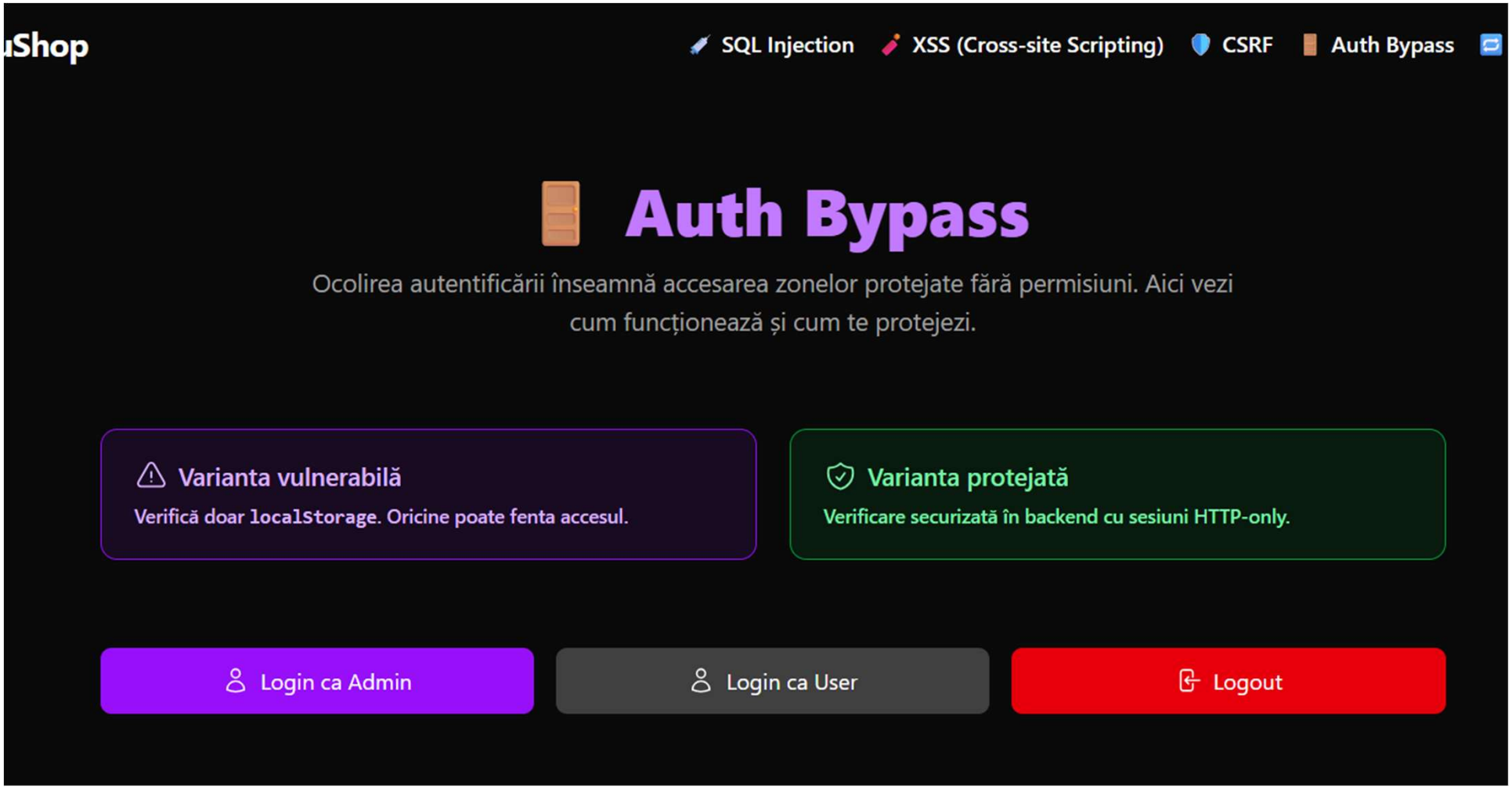
Niciun transfer efectuat în această sesiune.

🔐 **De ce iframe-ul malițios NU mai funcționează?**

Atacurile CSRF se bazează pe trimiterea automată a cookie-urilor. Dar acum cererea este respinsă pentru că **lipsește tokenul CSRF**, iar un site extern NU îl poate obține.

```
ForbiddenError: invalid csrf token
    at csrf (C:\Users\balan\Documents\GitHub\SecuShop\server\node_modules\csurf\index.js:112:19)
    at Layer.handleRequest (C:\Users\balan\Documents\GitHub\SecuShop\server\node_modules\router\lib\lay
    at next (C:\Users\balan\Documents\GitHub\SecuShop\server\node_modules\router\lib\route.js:157:13)
    at cookieParser (C:\Users\balan\Documents\GitHub\SecuShop\server\node_modules\cookie-parser\index.j
```

Această iframe încearcă să trimită cererea, dar serverul o respinge automat.


uShop
SQL Injection
XSS (Cross-site Scripting)
CSRF
Auth Bypass
Auth Bypass
Ocolirea autentificării înseamnă accesarea zonelor protejate fără permisiuni. Aici vezi cum funcționează și cum te protejezi.
Varianta vulnerabilă
Verifică doar localStorage. Oricine poate fenta accesul.
Varianta protejată
Verificare securizată în backend cu sesiuni HTTP-only.
Login ca Admin
Login ca User
Logout

Navigare admin

- Dashboard
- Comenzi
- Utilizatori
- Setări sistem

✅ Ai acces complet la dashboard

Sistemul crede că ești admin doar pentru că ai setat `localStorage` . Nu există verificare reală!

Comenzi active	Utilizatori înregistrați	Venit lunar
12	**487**	**34.500 RON**

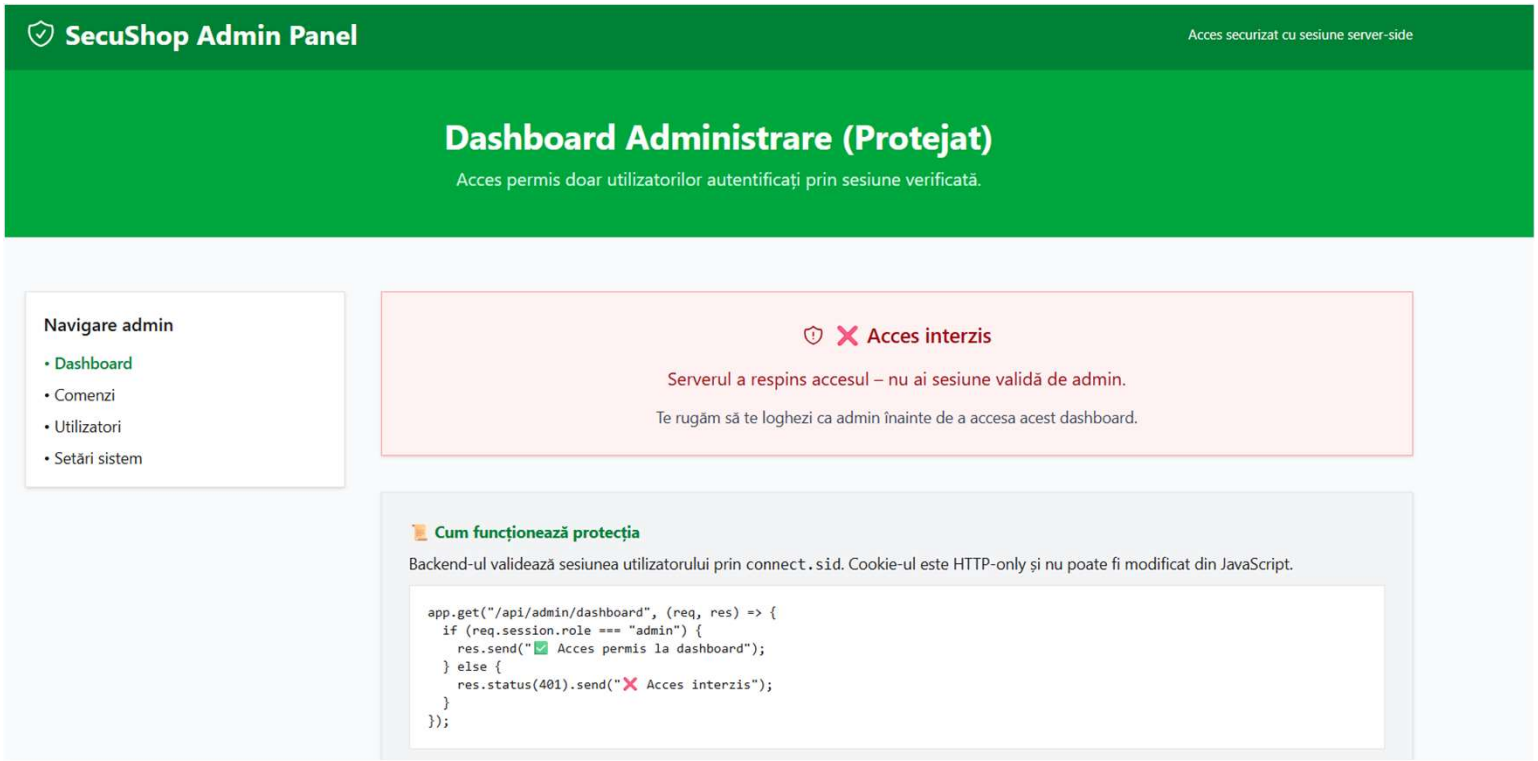
🔧 Control administrativ critic

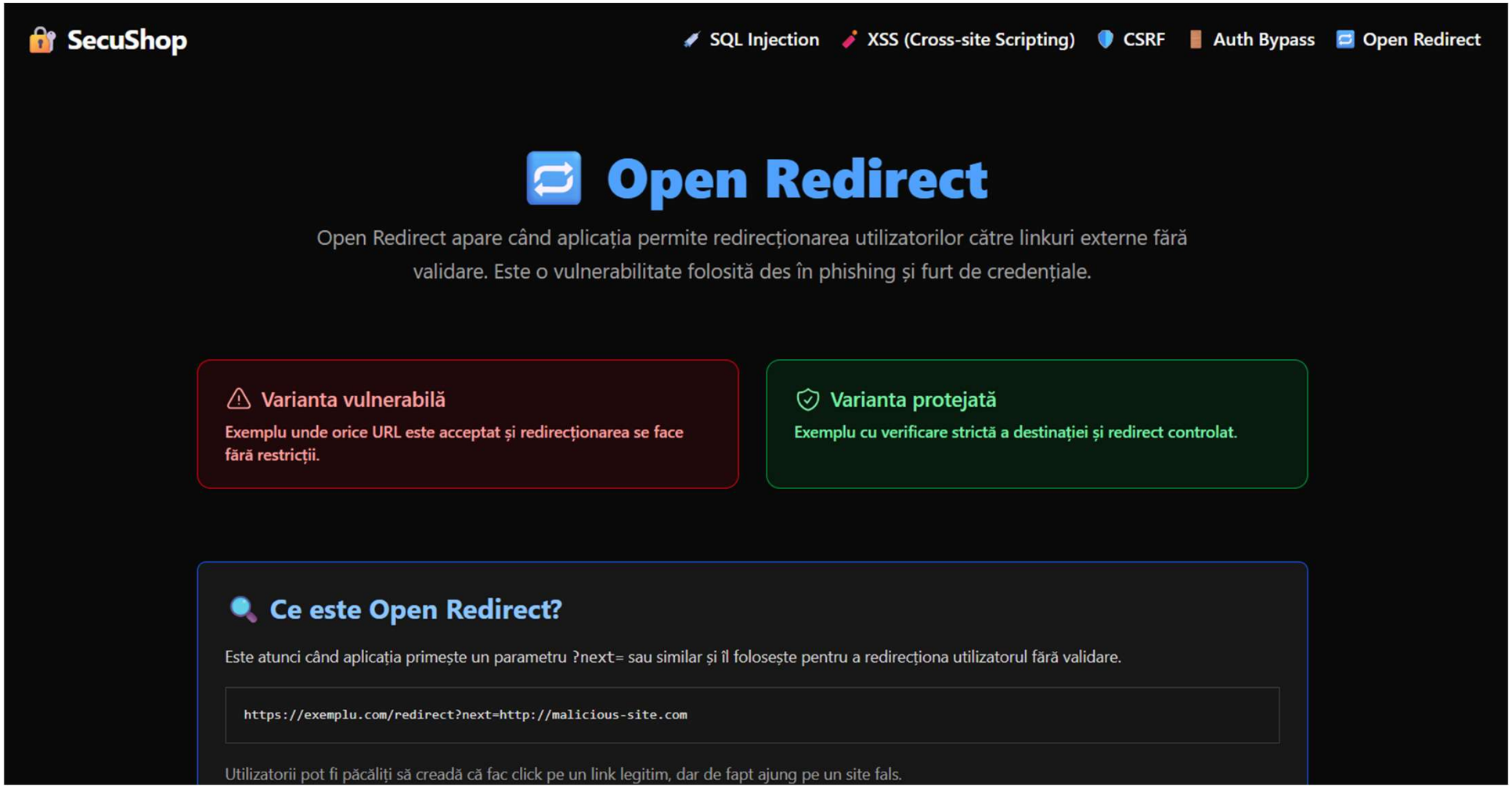
Acest buton ar putea șterge date sau reseta serverul. Și totul e accesibil fără autentificare reală.

🚨 Șterge toate comenzile (exemplu periculos)

📜 Cod frontend vulnerabil

```
const role = localStorage.getItem("role");
if (role === "admin") {
  setIsAdmin(true);
}
```


SecuShop Admin Panel
Acces securizat cu sesiune server-side
Dashboard Administrare (Protejat)
Acces permis doar utilizatorilor autentificați prin sesiune verificată.
Navigare admin
• Dashboard
• Comenzi
• Utilizatori
• Setări sistem
❌ Acces interzis
Serverul a respins accesul – nu ai sesiune validă de admin.
Te rugăm să te loghezi ca admin înainte de a accesa acest dashboard.
Cum funcționează protecția
Backend-ul validează sesiunea utilizatorului prin connect.sid. Cookie-ul este HTTP-only și nu poate fi modificat din JavaScript.
app.get("/api/admin/dashboard", (req, res) => {
if (req.session.role === "admin") {
res.send("✅ Acces permis la dashboard");
} else {
res.status(401).send("❌ Acces interzis");
}
});


SecuShop
SQL Injection
XSS (Cross-site Scripting)
CSRF
Auth Bypass
Open Redirect
Open Redirect
Open Redirect apare când aplicația permite redirecționarea utilizatorilor către linkuri externe fără validare. Este o vulnerabilitate folosită des în phishing și furt de credențiale.
Varianta vulnerabilă
Exemplu unde orice URL este acceptat și redirecționarea se face fără restricții.
Varianta protejată
Exemplu cu verificare strictă a destinației și redirect controlat.
Ce este Open Redirect?
Este atunci când aplicația primește un parametru ?next= sau similar și îl folosește pentru a redirecționa utilizatorul fără validare.
https://exemplu.com/redirect?next=http://malicious-site.com
Utilizatorii pot fi păcăliți să creadă că fac click pe un link legitim, dar de fapt ajung pe un site fals.

SecuShop Checkout

1 produs în coș

Atenție: Redirect Vulnerabil

Această pagină redirecționează utilizatorii către orice URL primit prin parametru.

Comandă

- Coșul tău
- Adresă livrare
- Plata
- Autentificare (Vulnerabil)

Conectare cont (Vulnerabil)

După autentificare, vei fi redirecționat către URL-ul specificat. Un atacator poate modifica acest URL pentru a te trimite către un site malițios.

Email

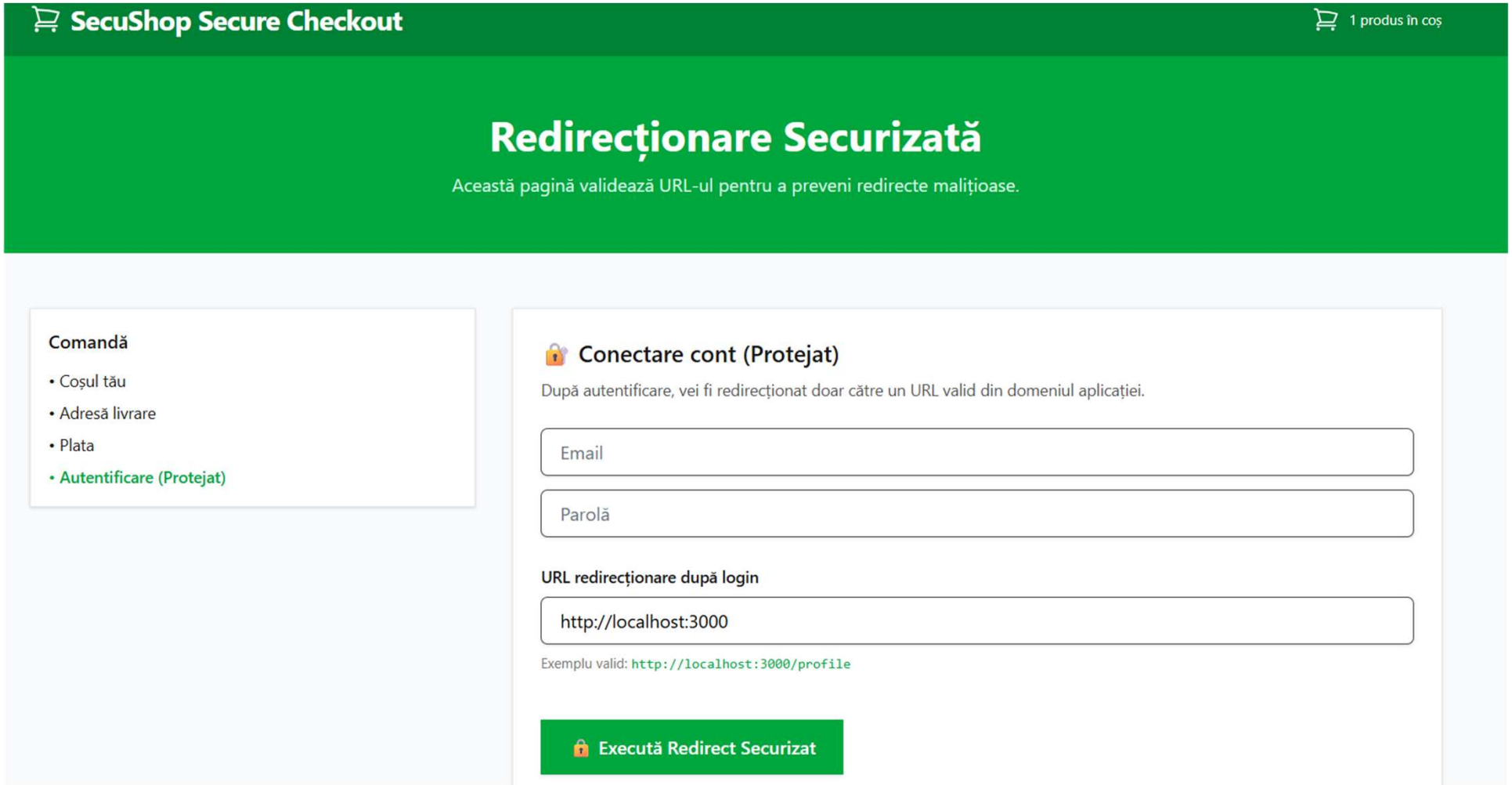
Parolă

URL redirecționare după login

http://localhost:3000

Exemplu periculos: `http://malicious.com`

Execută Redirect Vulnerabil


SecuShop Secure Checkout
1 produs în coș
Redirecționare Securizată
Această pagină validează URL-ul pentru a preveni redirecte malițioase.
Comandă
• Coșul tău
• Adresă livrare
• Plata
• Autentificare (Protejat)
Conectare cont (Protejat)
După autentificare, vei fi redirecționat doar către un URL valid din domeniul aplicației.
Email
Parolă
URL redirecționare după login
http://localhost:3000
Exemplu valid: http://localhost:3000/profile
Execută Redirect Securizat