

Acces privat pe resurse proprii

Fișă publică de proiect · exerciții și criterii de acceptare

Construiești o matrice de permisiuni pentru documente. Accentul este pe diferența dintre login, email verificat și autorizarea resursei.

Livrabile

- Matrice de acces
- Flux login
- Policy
- Teste cu două conturi

Criterii de acceptare

- Alt cont nu citește documentul
- Emailul neverificat este tratat conform regulii
- Logout invalidează sesiunea

Autentificare, autorizare și validare în trei verificări

Autentificarea răspunde cine face cererea, autorizarea dacă poate face operația, iar validarea dacă datele au forma acceptată. Niciuna nu le înlocuiește pe celelalte. O cerere a unui utilizator autentificat poate fi refuzată pentru resursa altuia, chiar dacă payloadul este valid. Separă cele trei teste ca să poți localiza defectul. Nu folosi un câmp role sau user_id trimis de browser drept dovadă de drepturi.

Exemplu de lucru

Matrice:

Vizitator + payload valid → autentificare cerută.

User B + resursa lui A + payload valid → refuz acces.

User A + resursa lui A + payload invalid → eroare validare.

User A + resursa lui A + payload valid → succes.

Dovada succesului: răspuns corect și modificare DB permisă.

Interpretarea rezultatului

Matricea trebuie aplicată și endpointurilor mai puțin vizibile, precum export și descărcare. Ascunderea unui buton nu schimbă drepturile serverului. Verifică resursa după refuz pentru a demonstra că nu a fost modificată parțial.

Exercițiu de consolidare

Aplică matricea unui endpoint de descărcare PDF privat și descrie ce se întâmplă la o cerere directă fără cont.

1. Modelul de securitate

Aplică matricea unui endpoint de descărcare PDF privat și descrie ce se întâmplă la o cerere directă fără cont.

Verificare orientativă

Matricea trebuie aplicată și endpointurilor mai puțin vizibile, precum export și descărcare. Ascunderea unui buton nu schimbă drepturile serverului. Verifică resursa după refuz pentru a demonstra că nu a fost modificată parțial.

De evitat

Rolul din interfață nu trebuie acceptat de server ca adevăr.

Flux complet de login și reset în laborator

Un starter kit oferă componente întreținute, dar instalarea nu încheie verificarea. Testează înregistrarea, autentificarea, ieșirea și resetarea parolei cu un mailer de laborator. Nu trimite mesaje reale către adrese inventate sau străine. Păstrează mesajele publice prudente pentru a nu dezvălui inutil existența conturilor. Configurația de sesiune, HTTPS și limitarea încercărilor trebuie verificată în mediul public.

Exemplu de lucru

Pentru proiectul didactic Laravel 11, verifică documentația starter kitului compatibil înainte de instalare.

Scenarii: parolă greșită; login valid; logout; link reset invalid; link reset folosit; login cu parola nouă.

Mail de test: fake sau log local, fără expediere externă.

Nu păstra: parole în loguri sau fixtures reale.

Interpretarea rezultatului

Un reset reușit trebuie să schimbe efectiv parola și să respecte politica sesiunilor. Captura unui formular frumos nu dovedește funcționarea fluxului. Verifică și ce se întâmplă după expirarea sau reutilizarea linkului, conform configurării alese.

Exercițiu de consolidare

Scrie un test care demonstrează că parola veche nu mai autentifică utilizatorul după reset.

2. Breeze: login, register, reset

Scrie un test care demonstrează că parola veche nu mai autentifică utilizatorul după reset.

Verificare orientativă

Un reset reușit trebuie să schimbe efectiv parola și să respecte politica sesiunilor. Captura unui formular frumos nu dovedește funcționarea fluxului. Verifică și ce se întâmplă după expirarea sau reutilizarea linkului, conform configurării alese.

De evitat

Exemplele vechi cu Breeze pot necesita adaptare la versiunea aleasă.

Email verificat ca stare distinctă

Un utilizator autentificat poate avea email neverificat. Dacă o zonă cere verificarea, aplică middleware-ul și contractul potrivit modelului, nu doar un mesaj în interfață. Linkul de verificare trebuie să aparțină utilizatorului și să respecte semnătura și expirarea configurate. În laborator, folosește notificări false pentru a inspecta fluxul fără a trimite mail. Nu marca emailul verificat doar pentru că browserul a vizitat o adresă arbitrară.

Exemplu de lucru

Modelul implementează MustVerifyEmail conform Laravel 11.
Rută privată: middleware(['auth', 'verified']).
Teste: guest; user neverificat; user verificat; link invalid; link pentru alt cont.
Stare DB: email_verified_at este null înainte și dată confirmată după flux valid.

Interpretarea rezultatului

Verificarea adresei nu dovedește identitatea legală a persoanei și nu acordă automat roluri administrative. Păstrează aceste afirmații distincte în produs. Pentru schimbarea emailului, decide explicit dacă verificarea trebuie resetată și testează regula.

Exercițiu de consolidare

Describe comportamentul după schimbarea adresei și verifică faptul că accesul dependent de verificare urmează noua stare.

3. Verificare email

Describe comportamentul după schimbarea adresei și verifică faptul că accesul dependent de verificare urmează noua stare.

Verificare orientativă

Verificarea adresei nu dovedește identitatea legală a persoanei și nu acordă automat roluri administrative. Păstrează aceste afirmații distincte în produs. Pentru schimbarea emailului, decide explicit dacă verificarea trebuie resetată și testează regula.

De evitat

Email verificat nu dovedește identitatea legală a persoanei.

Permisiuni pe operații, nu numai etichete de rol

Un rol este o grupare de drepturi, nu o autorizație universală. Definește întâi operațiile: citire, modificare, export și administrare. Un operator poate avea drept de citire fără drept de ștergere. Nu folosi un simplu is_admin împrăștiat în template-uri ca singură regulă. Centralizează decizia și păstrează teste pentru combinațiile importante. Schimbarea rolului trebuie să fie ea însăși o operație protejată.

Exemplu de lucru

Rol;Citire;Modificare;Export;Roluri
Cititor;da;nu;nu;nu
Operator;da;da;după regulă;nu
Administrator;da;da;după regulă;da
Resursă proprie/străină: verificare suplimentară după politica produsului.
Payload interzis publicului: role=administrator.

Interpretarea rezultatului

Matricea este demonstrativă și trebuie adaptată. Un administrator nu trebuie presupus scutit de toate controalele de date sau audit. Testează modificarea rolului prin cerere directă cu un utilizator fără drept, nu doar absența opțiunii în meniu.

Exercițiu de consolidare

Adaugă un rol suport numai pentru citire și verifică separat endpointul de export.

4. Roluri și permisiuni

Adaugă un rol suport numai pentru citire și verifică separat endpointul de export.

Verificare orientativă

Matricea este demonstrativă și trebuie adaptată. Un administrator nu trebuie presupus scutit de toate controalele de date sau audit. Testează modificarea rolului prin cerere directă cu un utilizator fără drept, nu doar absența opțiunii în meniu.

De evitat

Un rol larg de admin dat implicit încalcă principiul accesului minim.

Policy aplicată înaintea modificării

Politica de update trebuie invocată pe resursa concretă înaintea schimbării. Validarea poate fi efectuată într-un Form Request, dar accesul și tranziția de stare rămân verificări distincte. Nu muta autorizarea după save, fiindcă datele ar putea fi deja modificate când refuzi răspunsul. Într-o operație cu mai multe scrieri, folosește o tranzacție după validarea drepturilor, potrivit contractului serviciului.

Exemplu de lucru

```
public function update(UpdateRequest $request, ServiceRequest $record) {
    Gate::authorize('update', $record);
    $record->update($request->validated());
    return new ServiceRequestResource($record->refresh());
}
```

Test refuz: salvează valoarea inițială → cerere user străin → 403 → aceeași valoare în DB.

Interpretarea rezultatului

refresh permite răspunsului să reflecte starea salvată. Nu include în validated câmpuri pe care operatorul nu are voie să le schimbe. Dacă aplicația folosește soft deletes sau scope-uri, verifică și felul în care model binding găsește resursa.

Exercițiu de consolidare

Scrie un test care verifică atât refuzul, cât și lipsa oricărei modificări în tabel.

5. Policies în practică

Scrie un test care verifică atât refuzul, cât și lipsa oricărei modificări în tabel.

Verificare orientativă

refresh permite răspunsului să reflecte starea salvată. Nu include în validated câmpuri pe care operatorul nu are voie să le schimbe. Dacă aplicația folosește soft deletes sau scope-uri, verifică și felul în care model binding găsește resursa.

De evitat

Testele pozitive singure nu verifică izolarea utilizatorilor.

Acces limitat și pentru liste, exporturi și fișiere

Protecția detaliului nu este suficientă dacă un export sau un fișier static expune aceleași date. Păstrează documentele private în storage nepublic și livrează-le printr-un endpoint care verifică drepturile. Identificatorii greu de ghicit nu sunt autorizare. Pentru listă, pornește din relația utilizatorului și verifică filtrarea. Pentru descărcare, testează atât URL-ul aplicației, cât și faptul că fișierul nu poate fi citit direct prin directorul public.

Exemplu de lucru

Listă: `$user->serviceRequests()->paginate(20)`.
Detaliu: policy pe model.
Export: aceeași limitare, nu toate rândurile.
Fișier: storage privat → controller → autorizare → download.
Teste: user A, user B, guest, resursă lipsă.
Cache: evită cache public pentru răspunsuri private.

Interpretarea rezultatului

Un răspuns privat poate fi expus și printr-o configurare greșită de cache. Verifică headerele și calea fizică a fișierului. Nu publica un link direct în /storage dacă accesul trebuie să rămână condiționat de cont sau achiziție.

Exercițiu de consolidare

Aplică verificările unui PDF cumpărat și confirmă că utilizatorul fără achiziție nu îl poate descărca prin niciuna dintre căi.

6. Acces pe resurse proprii

Aplică verificările unui PDF cumpărat și confirmă că utilizatorul fără achiziție nu îl poate descărca prin niciuna dintre căi.

Verificare orientativă

Un răspuns privat poate fi expus și printr-o configurare greșită de cache. Verifică headerele și calea fizică a fișierului. Nu publica un link direct în /storage dacă accesul trebuie să rămână condiționat de cont sau achiziție.

De evitat

Filtrarea listei nu protejează automat pagina de detaliu.

Atelier final: Matrice de acces pentru documente

Timp de lucru estimat: 40 de minute. Folosește datele de laborator de mai jos și salvează rezultatul separat de orice proiect real.

Date de pornire

Documentul D1 aparține lui A, D2 lui B. Contul C are email neverificat. Vizitatorul nu este autentificat. Regula laboratorului: numai proprietarul cu email verificat poate descărca.

1. Pregătire — 5 minute

Extrage intrările și condițiile din enunț. Notează ce rezultat trebuie produs și ce informații nu sunt confirmate. Pregătește fișierele sau tabelul în care vei păstra dovada lucrului.

2. Construire — 15 minute

Construiește matricea celor patru identități pentru cele două documente. Implementează controlul pe ruta de descărcare și testează accesul direct la URL.

3. Variație și verificare — 15 minute

Schimbă proprietarul numai în fixture și repetă testele. Explică de ce protecția trebuie să citească relația reală, nu un ID trimis de solicitant.

4. Autoevaluare — 5 minute

Compară rezultatul cu reperele de mai jos. Înregistrează cel puțin o eroare identificată sau un caz-limită verificat, plus corectura ori explicația comportamentului observat.

Repere de rezolvare

A primește D1, B primește D2; accesul încrucișat, C și vizitatorul sunt refuzate conform contractului. Fișierul nu trebuie accesibil printr-un URL public alternativ.

Ce predai

- Matrice de acces
- Flux login
- Policy
- Teste cu două conturi

Criterii de acceptare

- Alt cont nu citește documentul
- Emailul neverificat este tratat conform regulii
- Logout invalidează sesiunea

Păstrează o versiune inițială și una revizuită, cu explicația diferențelor. Dacă un criteriu nu este îndeplinit, revino la lecția relevantă și repetă verificarea. Durata este orientativă; instalarea mediului și aprofundarea pot necesita timp suplimentar.

Registrul de lucru

Pentru fiecare etapă notează intrarea, rezultatul, dovada verificării, eroarea găsită și corectura. Nu introduce date personale sau secrete în fișa partajată.

Documentație și surse

- Documentația Laravel 11 — versiunea aplicației demonstrative — Laravel
- OWASP Top 10 — OWASP

<https://laravel.com/docs/11.x>

<https://owasp.org/projects/top-ten>