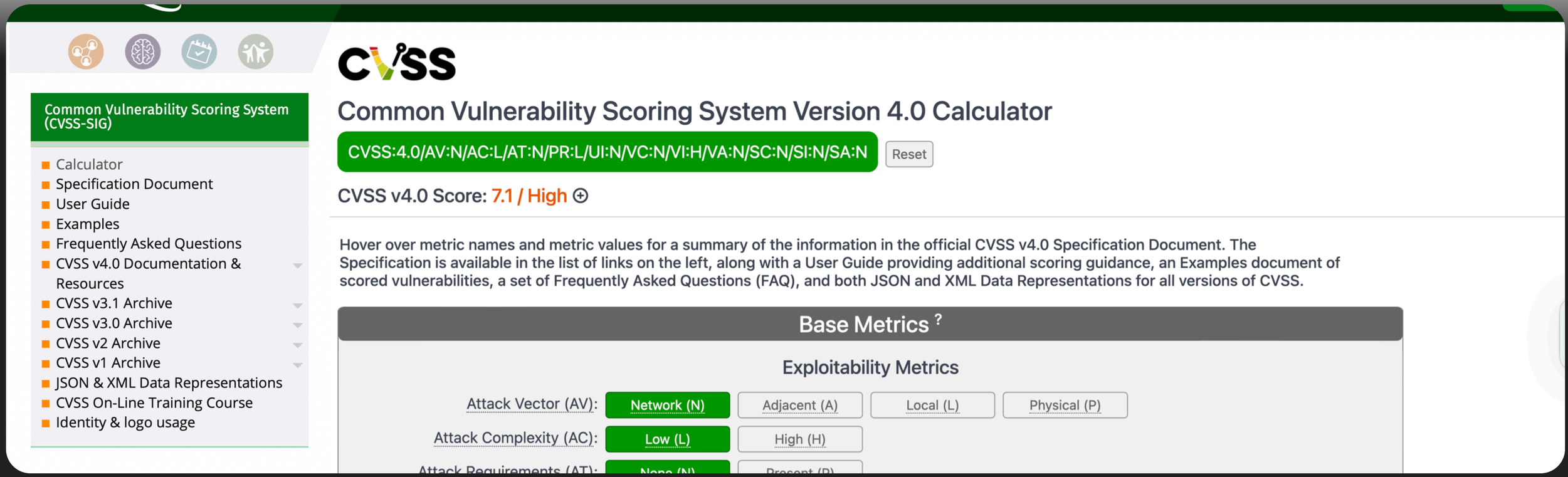
kelpompok 2

Finding Details: Faraj Muhiddin

CODE AUDITING

VULN - 001

BROKEN ACCESS CONTROL (IDOR) - CART QUANTITY MANIPULATION

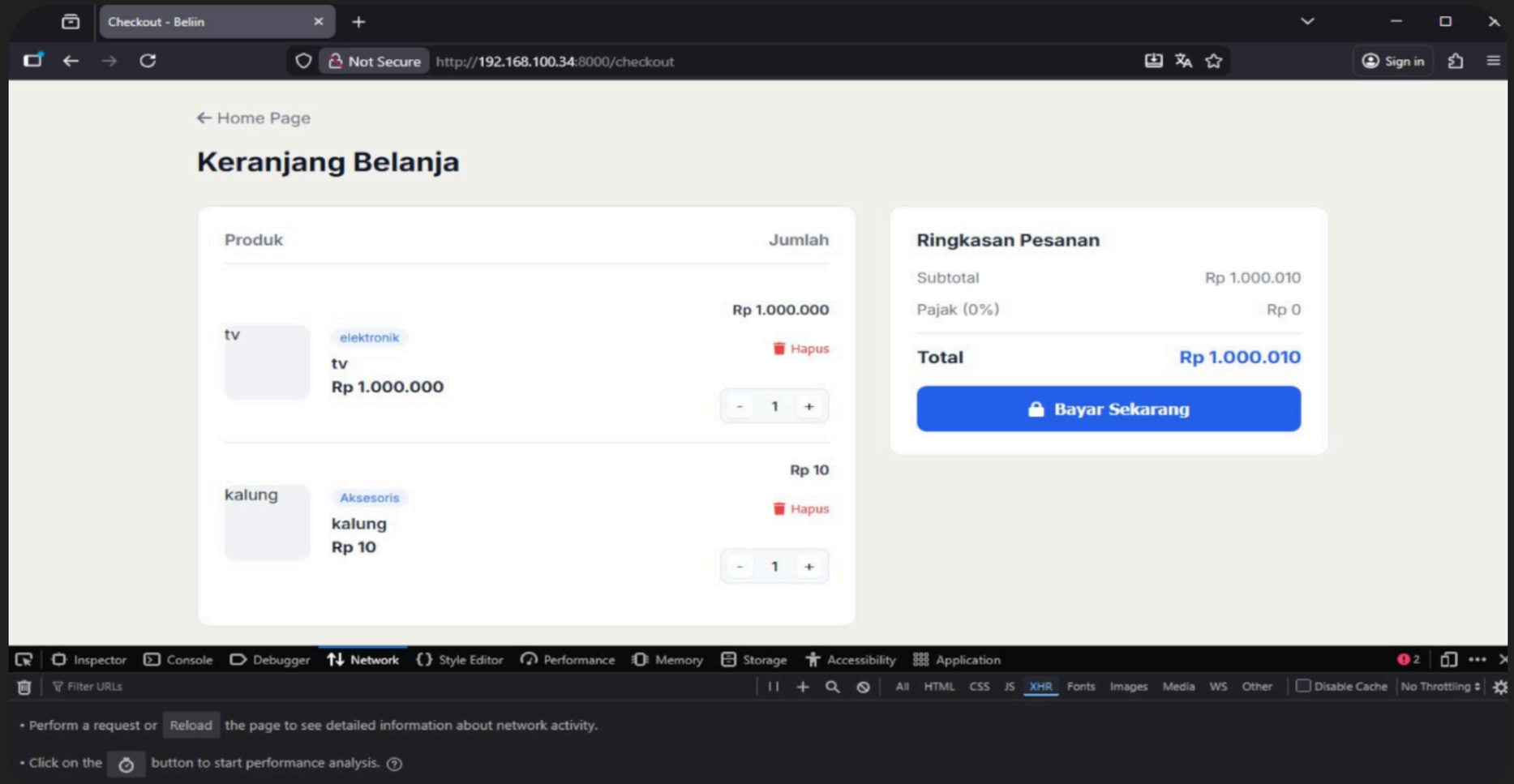


Broken Access Control (IDOR)

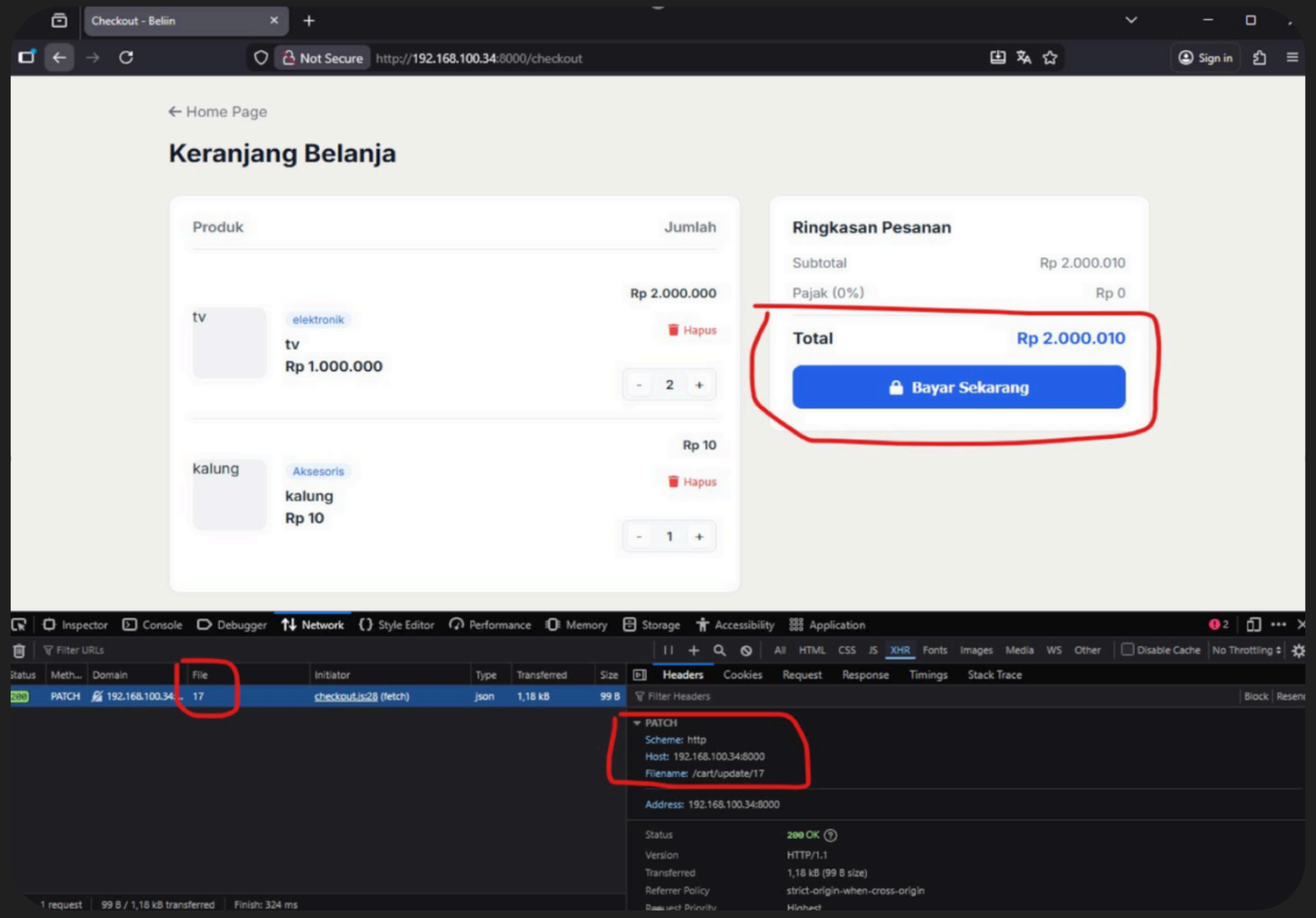
• Cart Quantity Manipulation

- *Executive Summary – Attacker dapat memodifikasi quntity item keranjang pada user lain dengan mengirim patch request ke endpoint tanpa verifikasi dari pemilik akun.*
- *CVSS Score – 7.1*
- *Severity – High*
- *CVSS String – CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N*

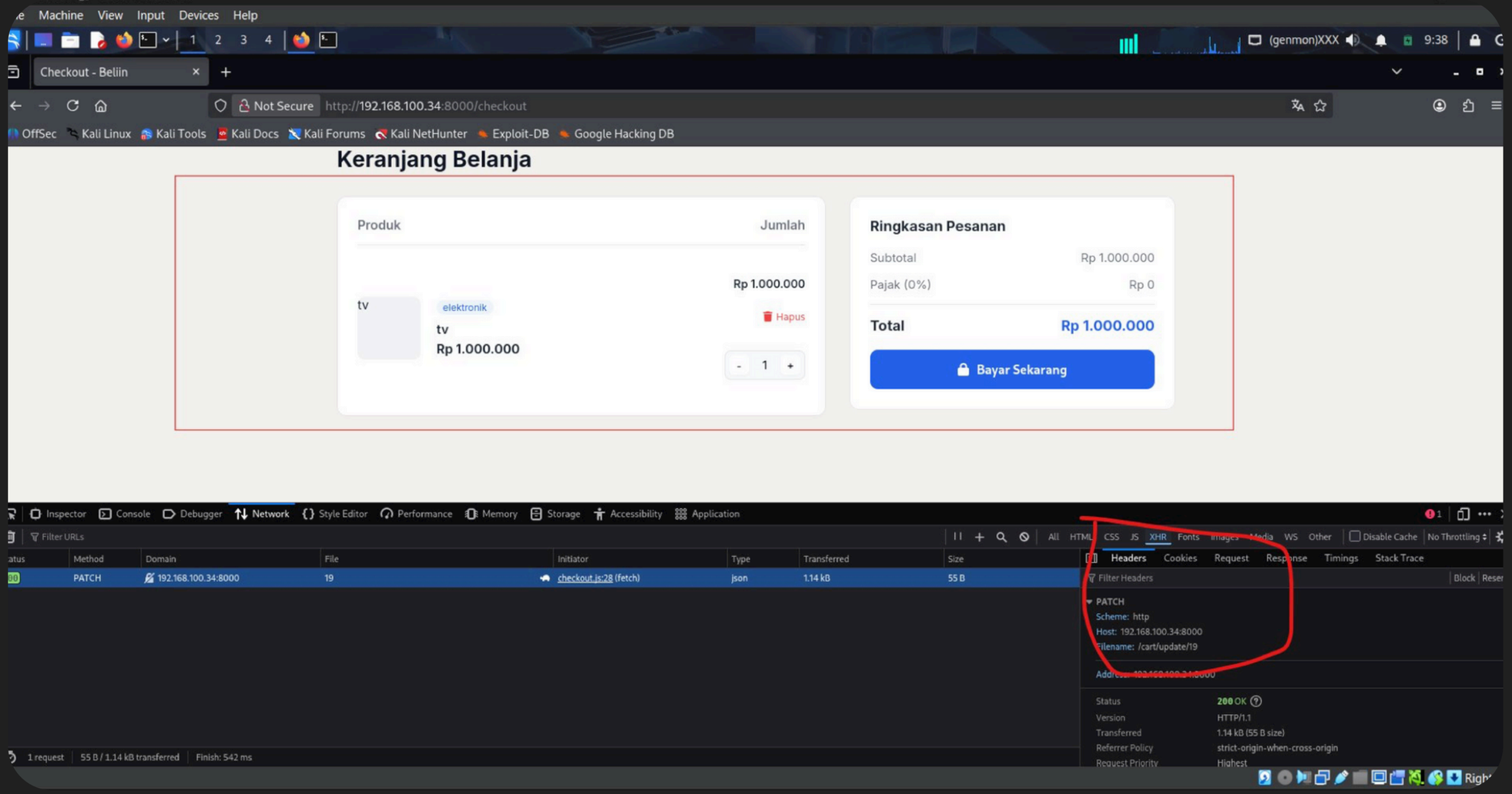
- **User Korban sebelum diubah quantity**



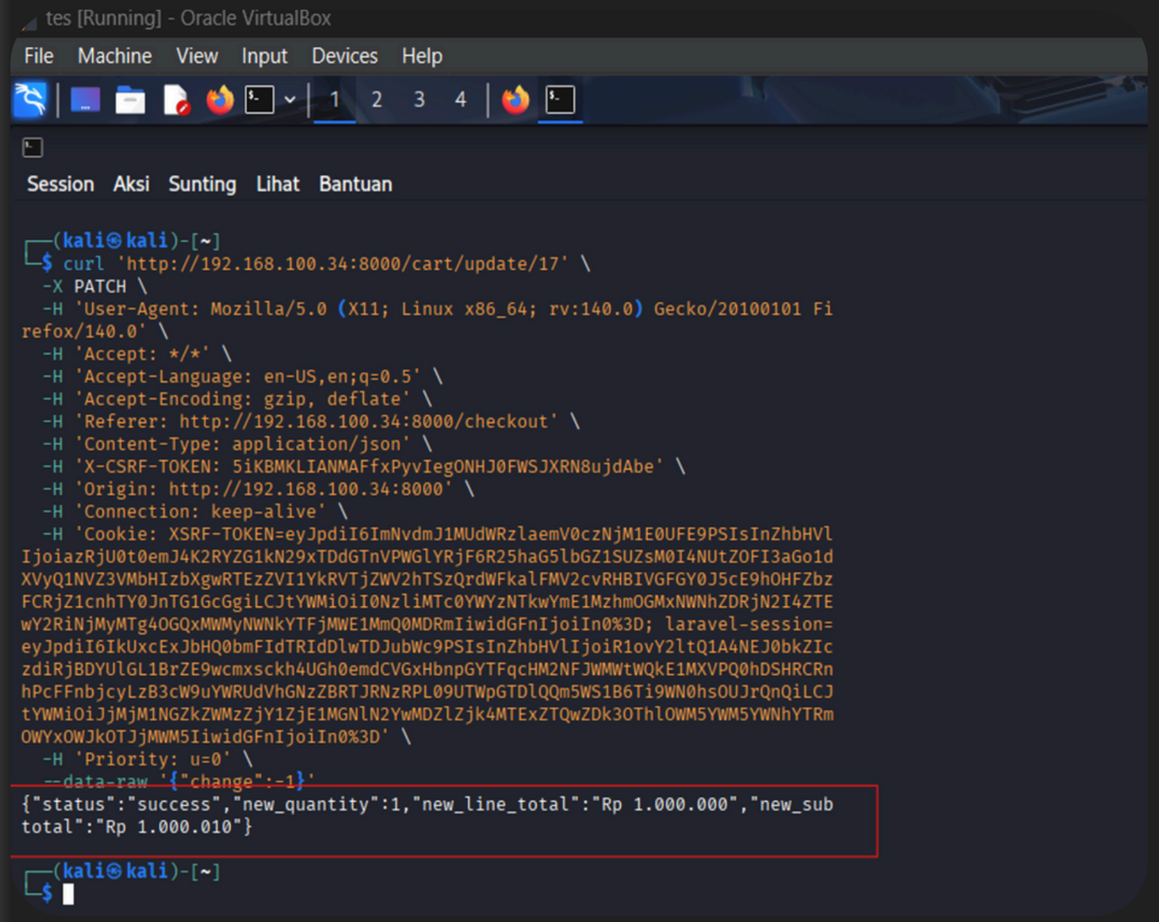
- **User Korban setelah diubah quantity**



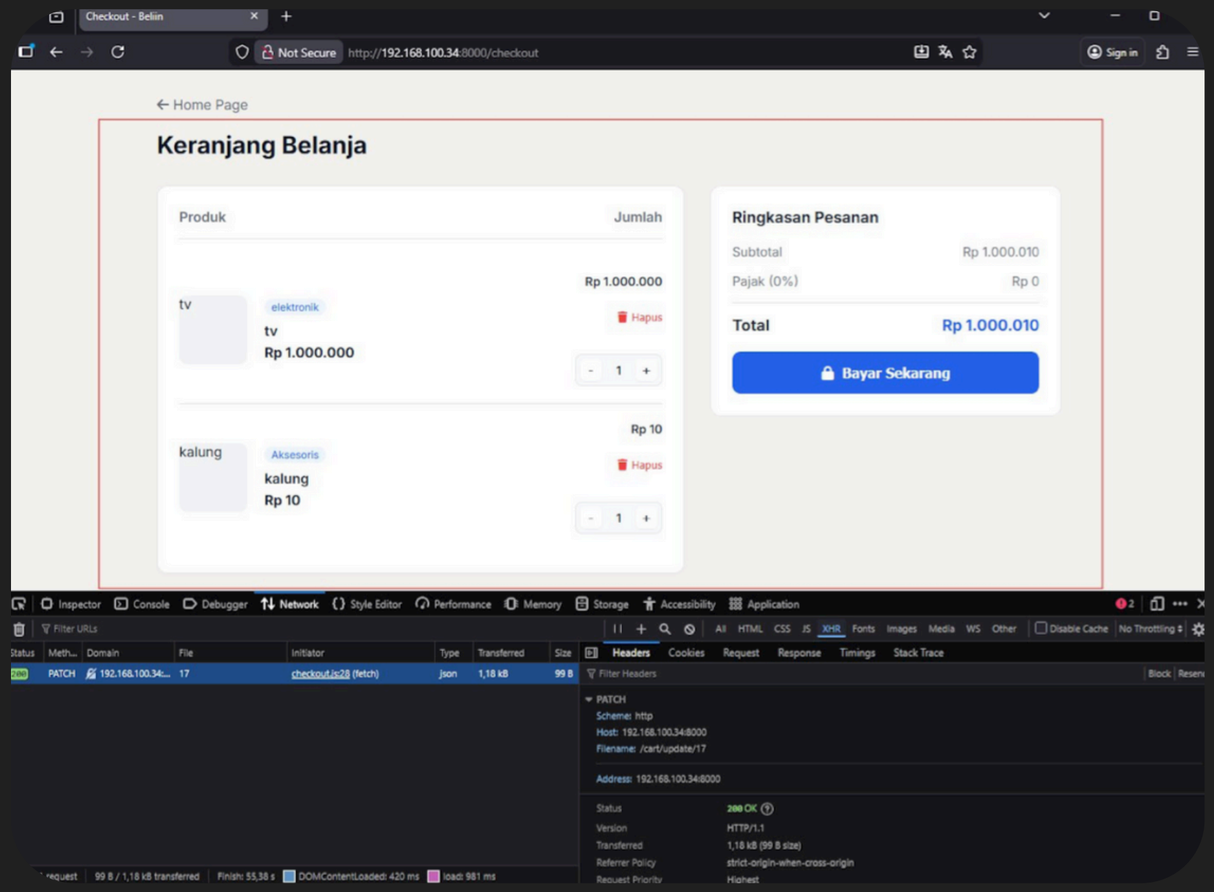
- **User penyerang login dan melihat id dari penyerang**



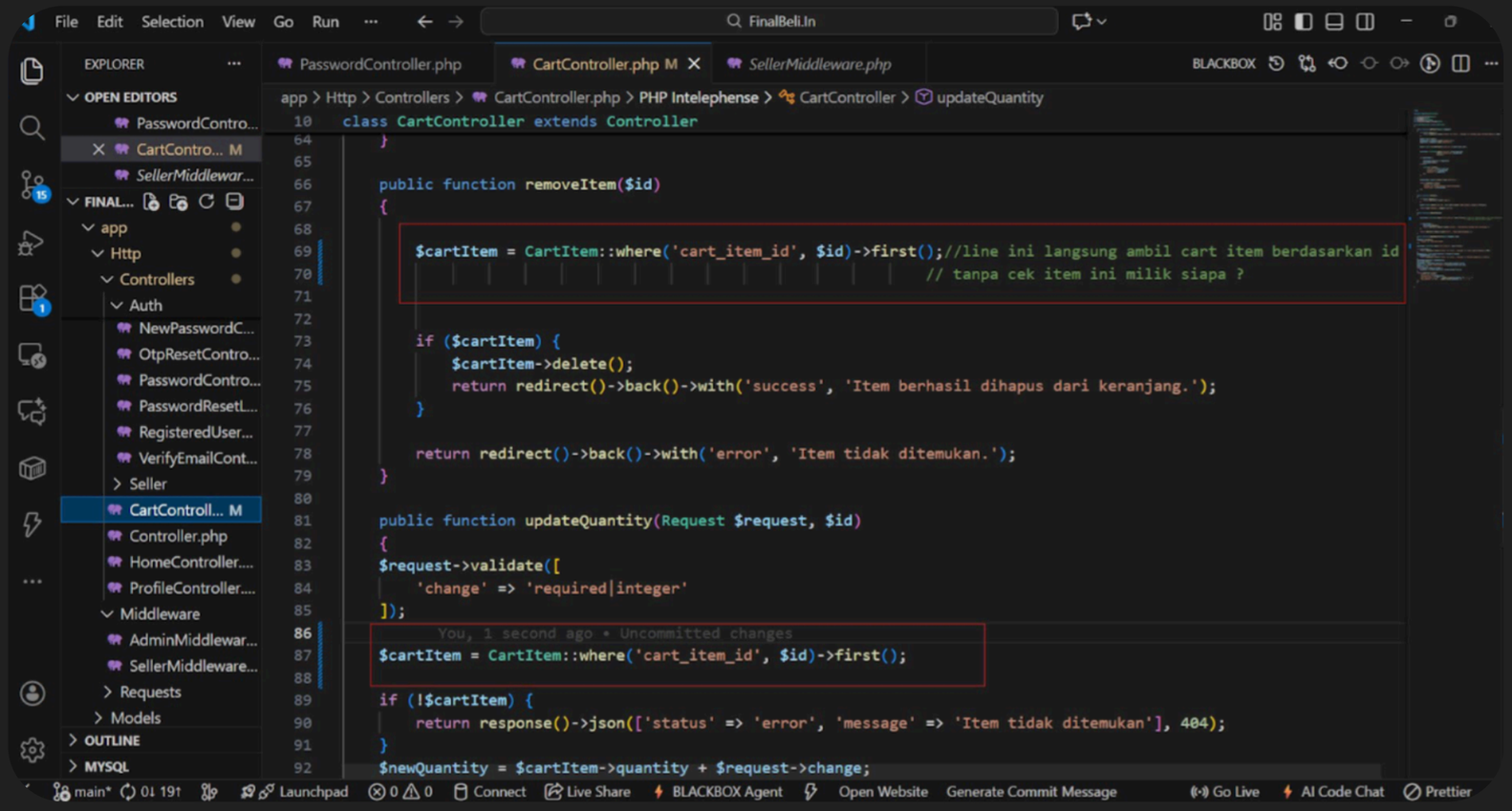
- penyerang mencoba attack melalui terminal kali dengan merubah idnya



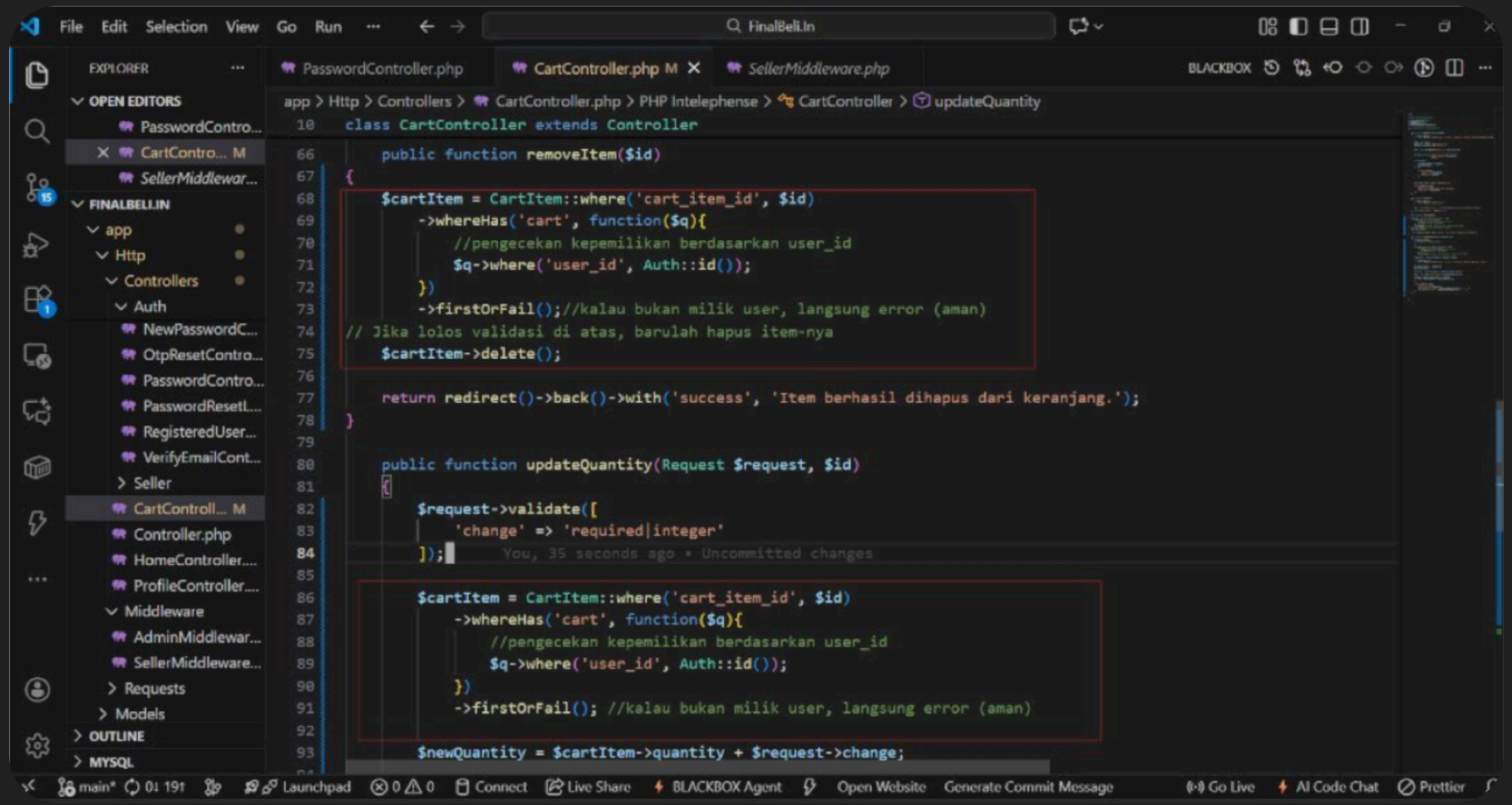
- Hasil user korban setelah di serang ini diserangnya untuk mengurangi cart



- kodingan yang salah pada removeItem dan updatequantity



- **Remediation Strategy – Tambahkan validasi user_id pada query, blokir akses unauthorized.**



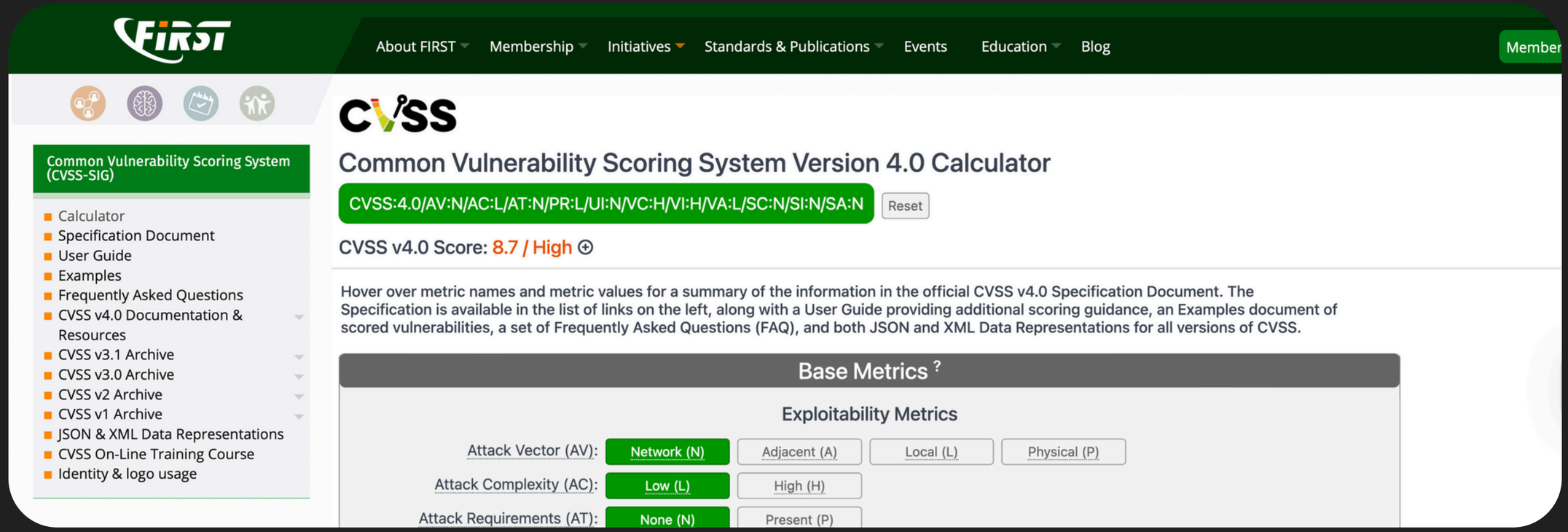
VULN - 002

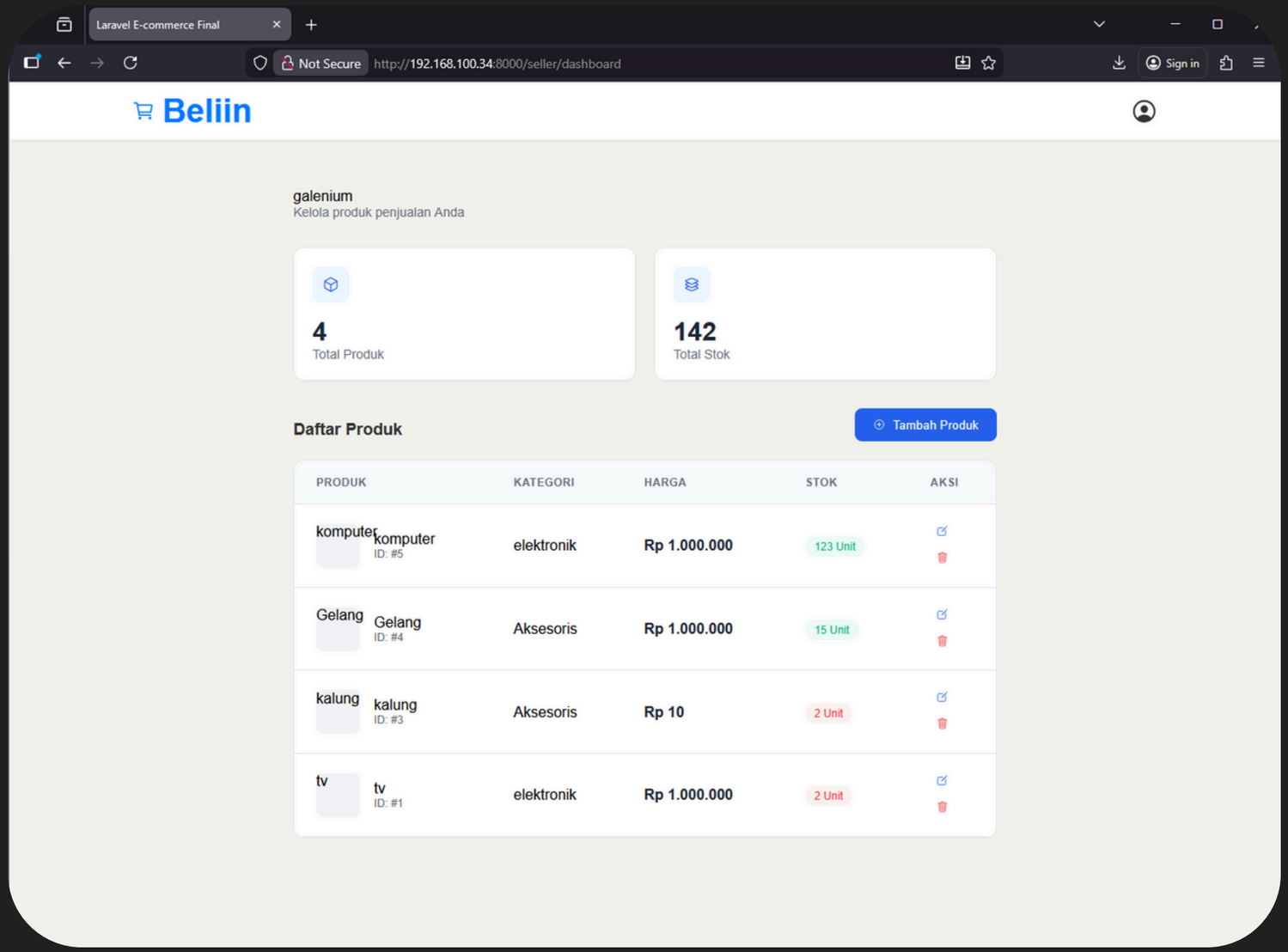
BROKEN ACCESS CONTROL (IDOR) – BOLA/IDOR ON SELLER PRODUCTS

Broken Access Control (IDOR)

- **BOLA/IDOR On Seller Products**

- *Executive Summary – Ditemukan bahwa role Seller dapat melihat, mengedit, dan menghapus produk milik seller lain tanpa validasi kepemilikan. Aplikasi gagal melakukan Object Ownership Validation sehingga menyebabkan Broken Object Level Authorization. Kerentanan ini memungkinkan sabotase bisnis antar seller karena seluruh aksi CRUD dapat dilakukan tanpa batasan user.*
- *CVSS Score – 8.7*
- *Severity – High*
- *CVSS String – CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N*




Laravel E-commerce Final
Not Secure
http://192.168.100.34:8000/seller/dashboard
Sign in
Beliin
galenium
Kelola produk penjualan Anda
4
Total Produk
142
Total Stok
Daftar Produk
Tambah Produk
PRODUK
KATEGORI
HARGA
STOK
AKSI
komputer
komputer
ID: #5
elektronik
Rp 1.000.000
123 Unit
Gelang
Gelang
ID: #4
Aksesoris
Rp 1.000.000
15 Unit
kalung
kalung
ID: #3
Aksesoris
Rp 10
2 Unit
tv
tv
ID: #1
elektronik
Rp 1.000.000
2 Unit

BROKEN ACCESS CONTROL (IDOR) – BOLA/IDOR ON SELLER PRODUCTS

Remediation Strategy :

- *Tambahkan kolom user_id pada tabel products.*
- *Filter produk di index:*
  where('user_id', Auth::id())
- *Validasi ownership pada update/delete:*
  where('user_id', Auth::id())firstOrFail()
- *Sembunyikan tombol edit/delete untuk produk non-owner.*

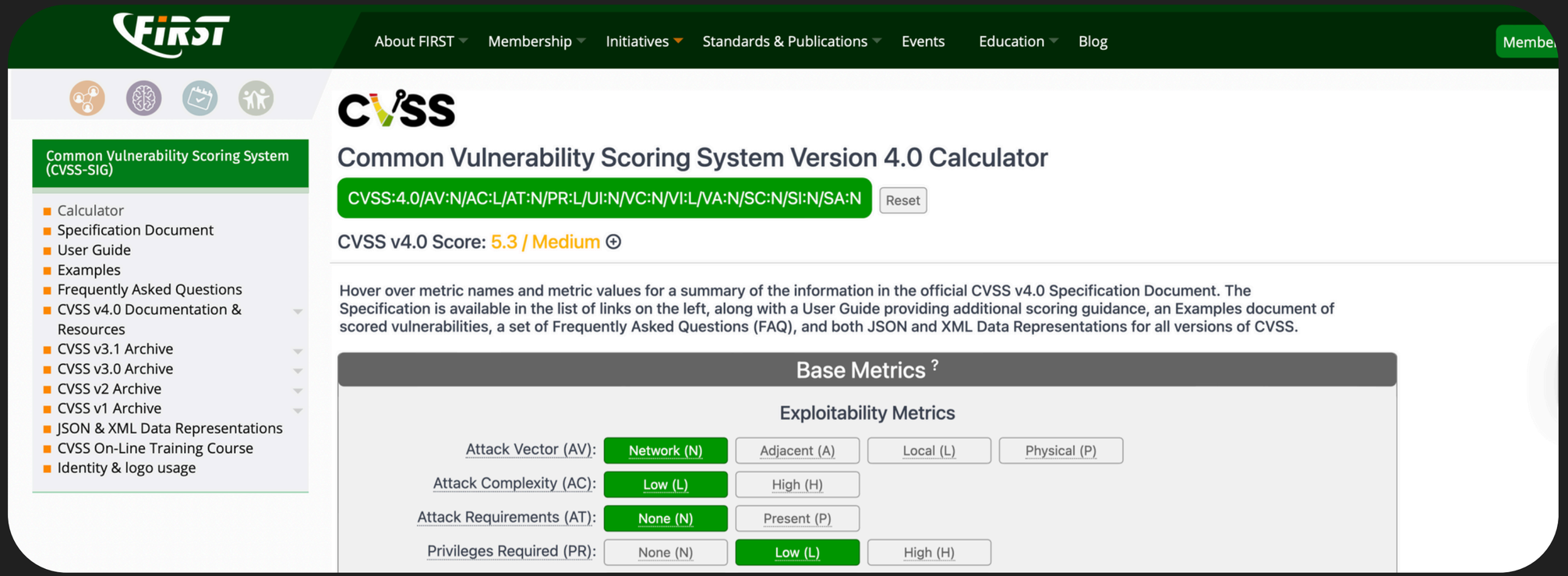
VULN - 003

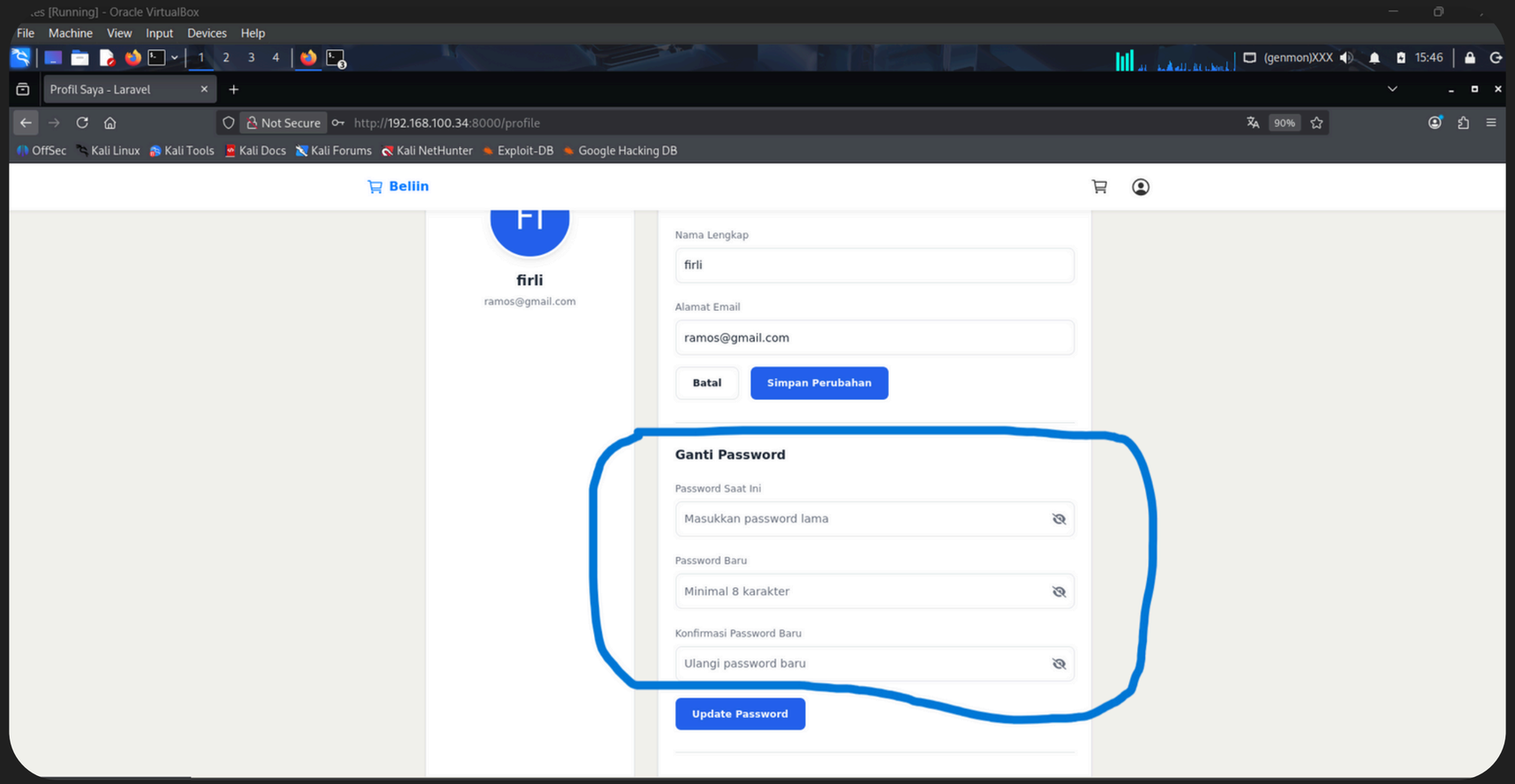
WEAK PASSWORD CHANGE POLICY (PASSWORD REUSE ALLOWED)

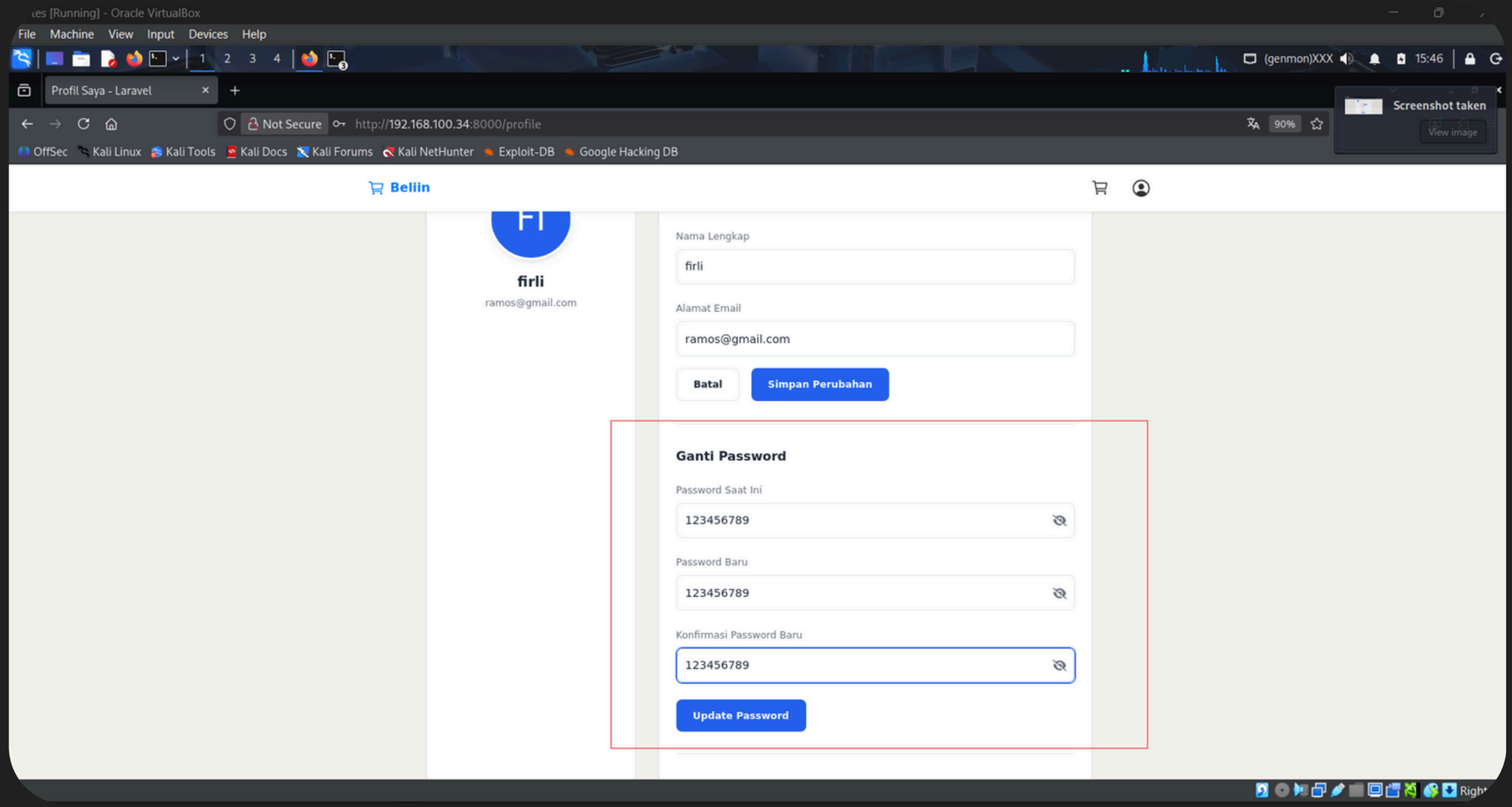
WEAK PASSWORD CHANGE POLICY

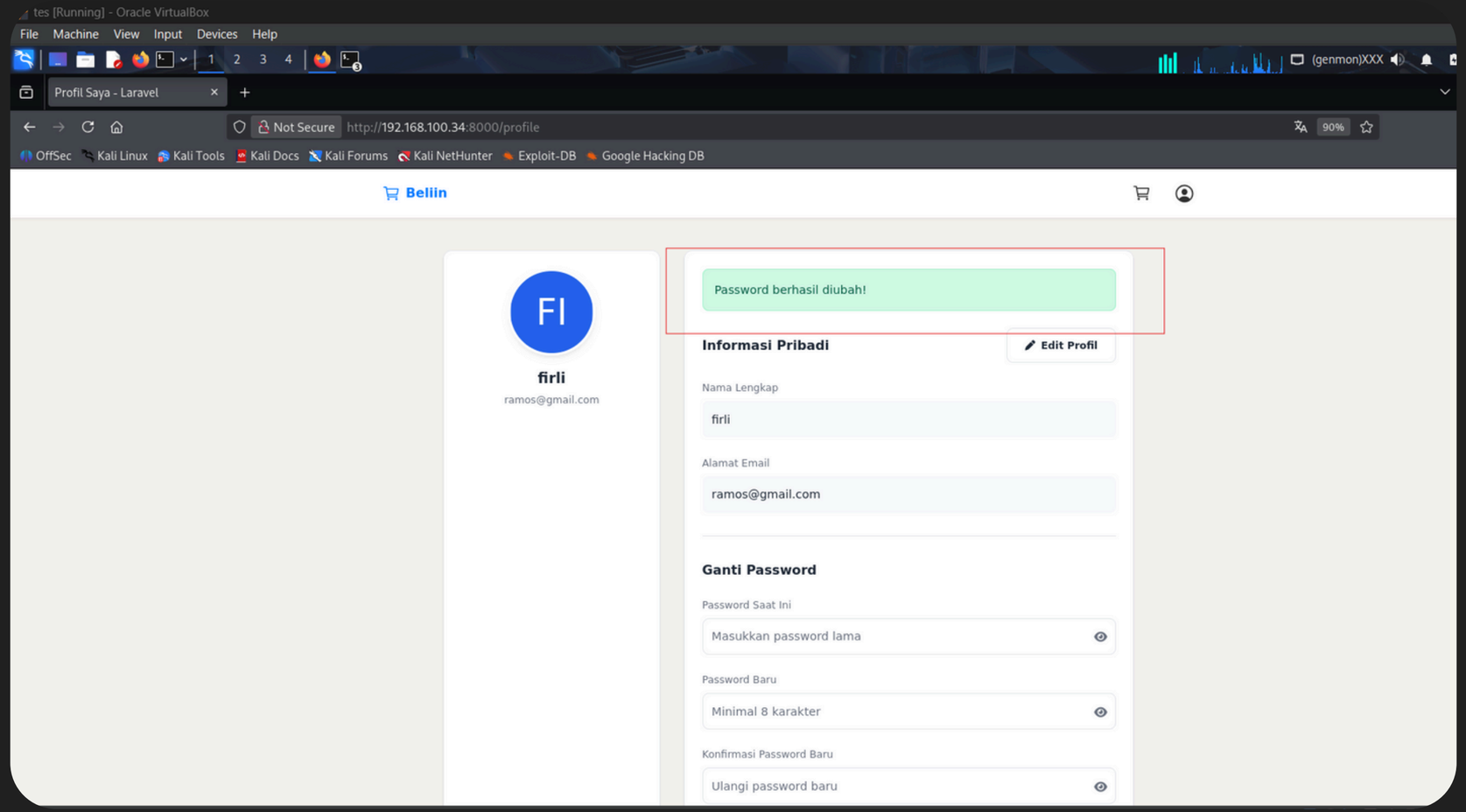
- **(PASSWORD REUSE ALLOWED)**

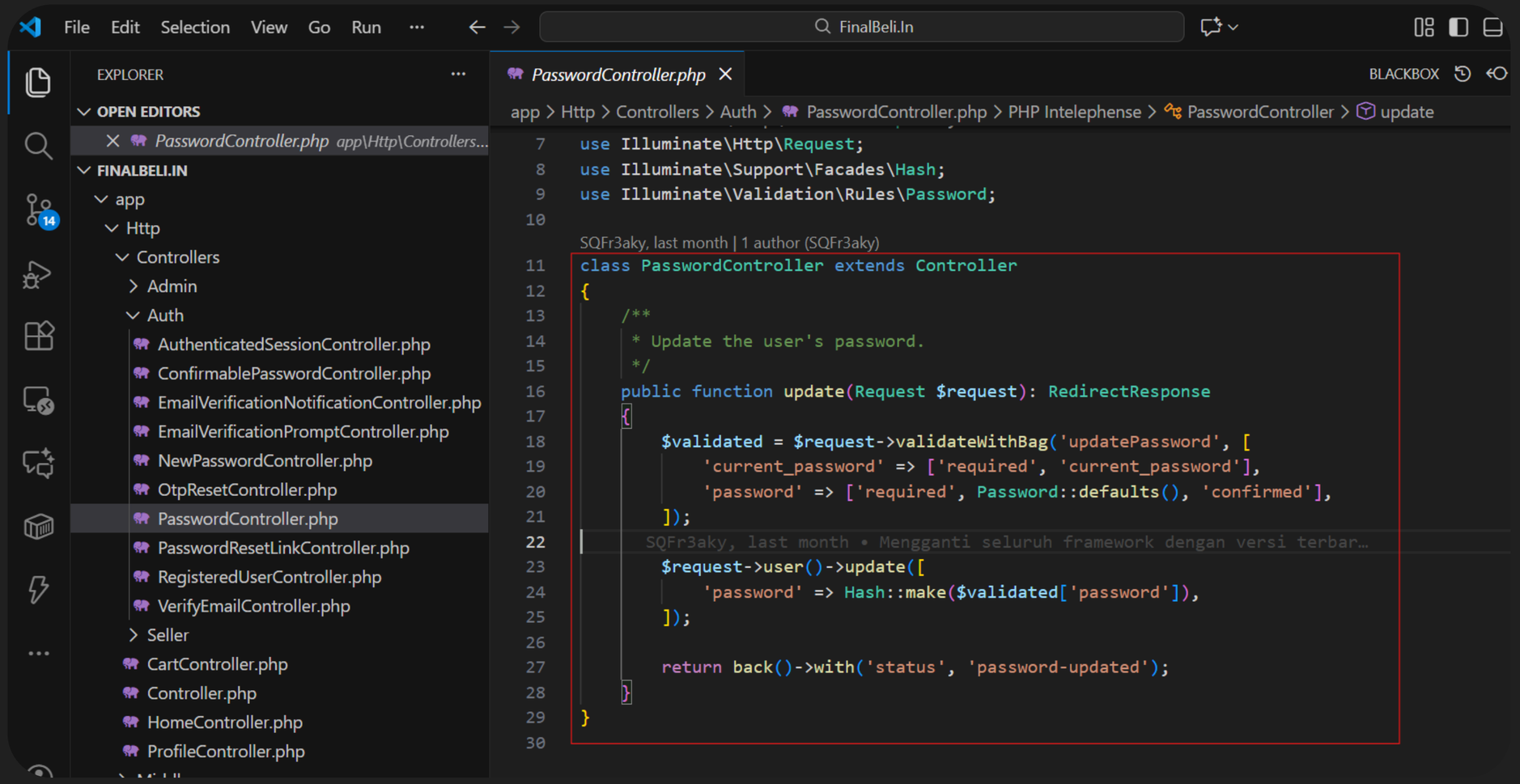
- *Executive Summary – Sistem mengizinkan pengguna mengubah password namun tetap menggunakan nilai password lama. Hal ini melemahkan keamanan credential lifecycle dan membuat rotasi password tidak efektif.*
- *CVSS Score – 5.3*
- *Severity – Medium*
- *CVSS String – CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N*




.es [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Profil Saya - Laravel
Not Secure http://192.168.100.34:8000/profile
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Belilin
FI
firli
ramos@gmail.com
Nama Lengkap
firli
Alamat Email
ramos@gmail.com
Batal
Simpan Perubahan
Ganti Password
Password Saat Ini
Masukkan password lama
Password Baru
Minimal 8 karakter
Konfirmasi Password Baru
Ulangi password baru
Update Password


es [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Profil Saya - Laravel
Not Secure http://192.168.100.34:8000/profile
Screenshot taken
View image
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Beliin
firli
ramos@gmail.com
Nama Lengkap
firli
Alamat Email
ramos@gmail.com
Batal
Simpan Perubahan
Ganti Password
Password Saat Ini
123456789
Password Baru
123456789
Konfirmasi Password Baru
123456789
Update Password


tes [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Profil Saya - Laravel
Not Secure http://192.168.100.34:8000/profile
90%
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Beliin
FI
firli
ramos@gmail.com
Password berhasil diubah!
Informasi Pribadi
Edit Profil
Nama Lengkap
firli
Alamat Email
ramos@gmail.com
Ganti Password
Password Saat Ini
Masukkan password lama
Password Baru
Minimal 8 karakter
Konfirmasi Password Baru
Ulangi password baru


File Edit Selection View Go Run
FinalBeli.In
EXPLORER
OPEN EDITORS
PasswordController.php app\Http\Controllers...
FINALBELI.IN
app
Http
Controllers
Admin
Auth
AuthenticatedSessionController.php
ConfirmablePasswordController.php
EmailVerificationNotificationController.php
EmailVerificationPromptController.php
NewPasswordController.php
OtpResetController.php
PasswordController.php
PasswordResetLinkController.php
RegisteredUserController.php
VerifyEmailController.php
Seller
CartController.php
Controller.php
HomeController.php
ProfileController.php
PasswordController.php
BLACKBOX
app > Http > Controllers > Auth > PasswordController.php > PHP Intelephense > PasswordController > update
use Illuminate\Http\Request;
use Illuminate\Support\Facades\Hash;
use Illuminate\Validation\Rules\Password;
SQFr3aky, last month | 1 author (SQFr3aky)
class PasswordController extends Controller
{
/**
* Update the user's password.
*/
public function update(Request $request): RedirectResponse
{
$validated = $request->validateWithBag('updatePassword', [
'current_password' => ['required', 'current_password'],
'password' => ['required', Password::defaults(), 'confirmed'],
]);
SQFr3aky, last month • Mengganti seluruh framework dengan versi terbar…
$request->user()->update([
'password' => Hash::make($validated['password']),
]);
return back()->with('status', 'password-updated');
}
}

WEAK PASSWORD CHANGE POLICY (PASSWORD REUSE ALLOWED)

Remediation Strategy

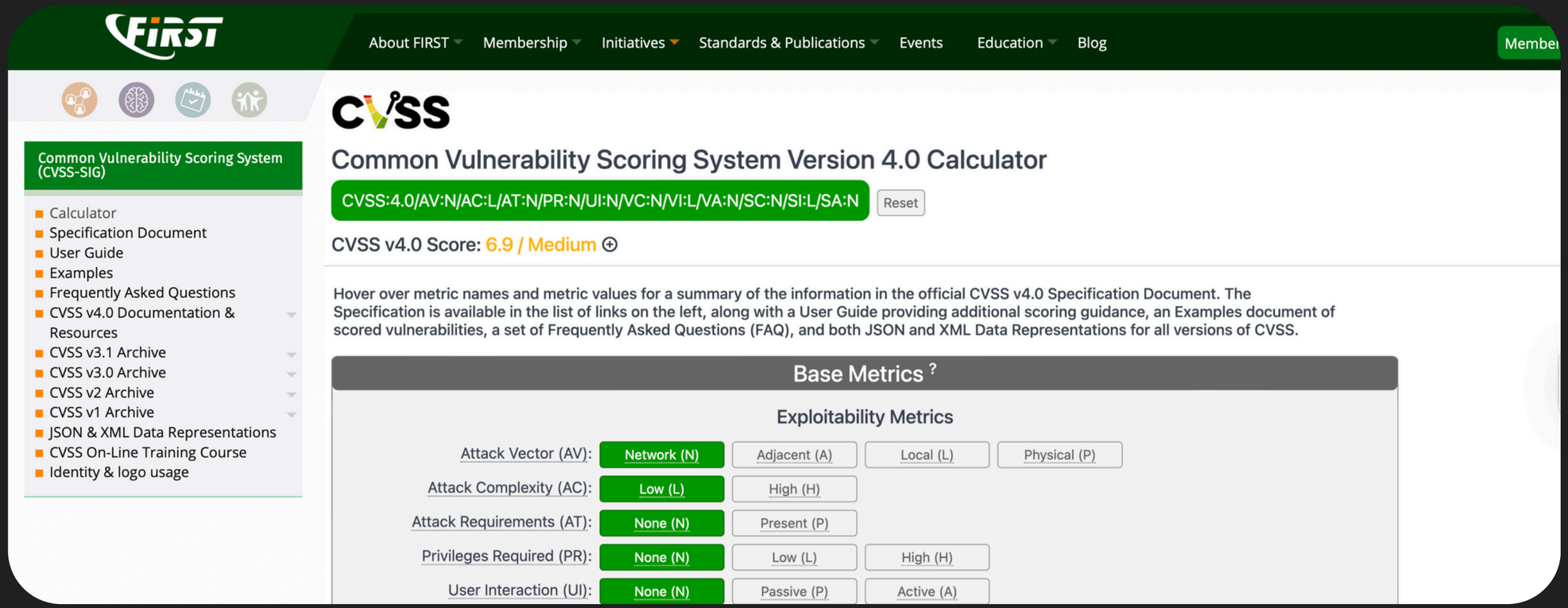
- *Tambahkan validasi untuk mencegah password baru sama dengan password lama,Pastikan password rotation policy diterapkan sesuai security best practice.*

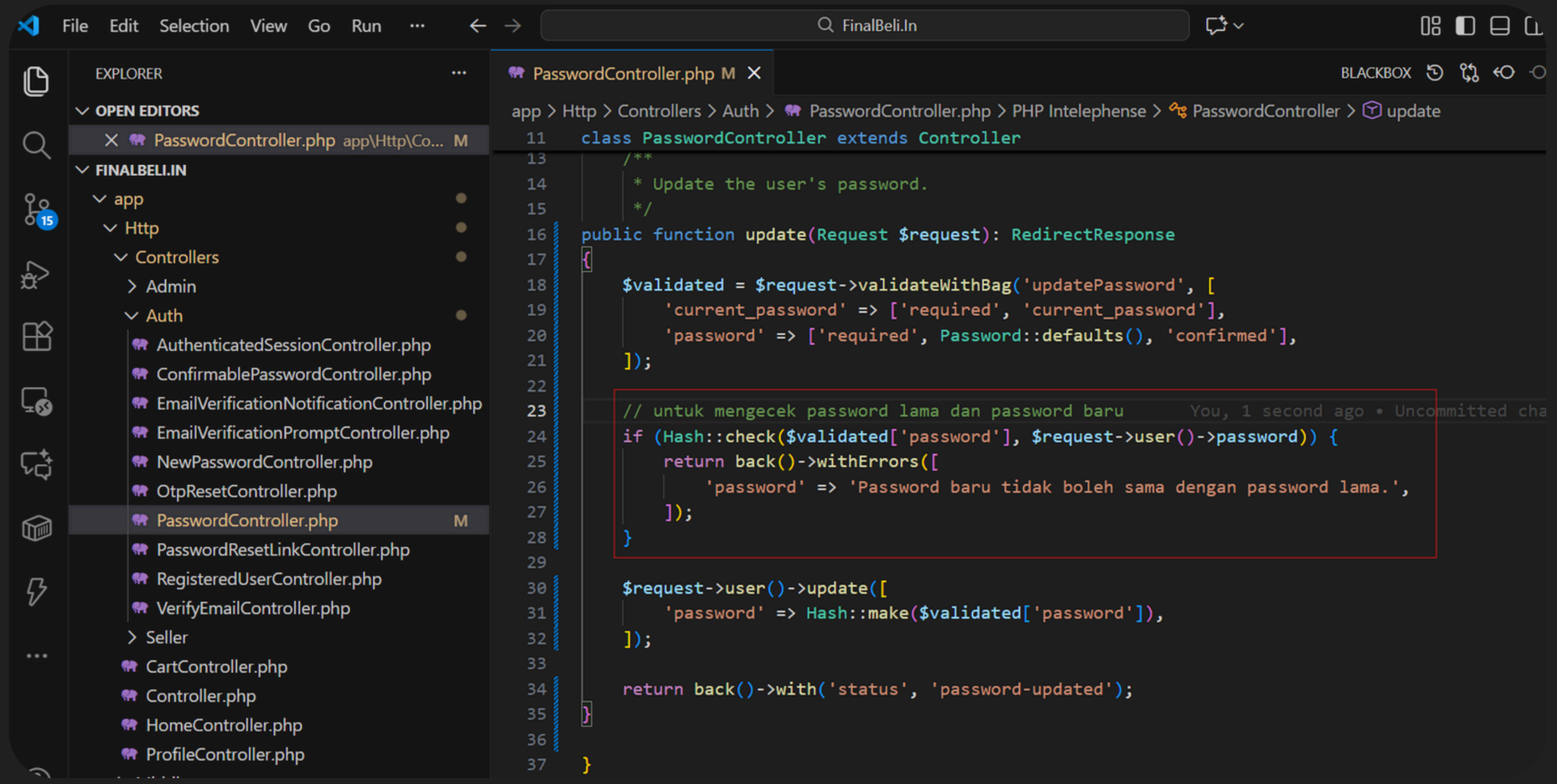
VULN - 004

WEAK PASSWORD POLICY

WEAK PASSWORD POLICY

- *Executive Summary – Sistem menggunakan password yang hanya mensyaratkan minimal 8 karakter tapi tidak mewajibkan kombinasi Huruf besar,kecil,angka,simbol. hal ini bisa menjadikan penyerang menggunakan passsword lemah sehingga kredensial pengguna mudah ditebak, meningkatkan resiko brute force.*
- *CVSS Score – 6.9*
- *Severity – Medium*
- *CVSS String – CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:L/SA:N*




File Edit Selection View Go Run
FinalBeli.In
EXPLORER
OPEN EDITORS
PasswordController.php app\Http\Co... M
FINALBELI.IN
app
Http
Controllers
Admin
Auth
AuthenticatedSessionController.php
ConfirmablePasswordController.php
EmailVerificationNotificationController.php
EmailVerificationPromptController.php
NewPasswordController.php
OtpResetController.php
PasswordController.php M
PasswordResetLinkController.php
RegisteredUserController.php
VerifyEmailController.php
Seller
CartController.php
Controller.php
HomeController.php
ProfileController.php
PasswordController.php M
BLACKBOX
app > Http > Controllers > Auth > PasswordController.php > PHP Intelephense > PasswordController > update
class PasswordController extends Controller
/**
* Update the user's password.
*/
public function update(Request $request): RedirectResponse
{
$validated = $request->validateWithBag('updatePassword', [
'current_password' => ['required', 'current_password'],
'password' => ['required', Password::defaults(), 'confirmed'],
]);
// untuk mengecek password lama dan password baru
You, 1 second ago • Uncommitted cha
if (Hash::check($validated['password'], $request->user()->password)) {
return back()->withErrors([
'password' => 'Password baru tidak boleh sama dengan password lama.',
]);
}
$request->user()->update([
'password' => Hash::make($validated['password']),
]);
return back()->with('status', 'password-updated');
}
}

WEAK PASSWORD CHANGE POLICY (PASSWORD REUSE ALLOWED)

Remediation Strategy :

1.Terapkan password policy yang lebih ketat di file RegisteredUserController.php

2. Tambahkan juga mitigasi bruteforce seperti rate limiting/login throttling

Security Programming

Thank You