White-Box Test Cases - Port Scanner

.

---

1. Authentication Module

Test ID	Function	Test Type	Condition / Path Tested	Expected Result
WB-AUTH-001	register()	Statement	Valid input → all lines executed	User added, OTP sent (201)
WB-AUTH-002	register()	Branch	Missing email/password → True path	400: "Email and password required"
WB-AUTH-003	register()	Branch	Duplicate email → add_user() returns None	409: "Email already registered"
WB-AUTH-004	verify_otp()	Condition	OTP valid & not expired → True path	User verified (200)
WB-AUTH-005	verify_otp()	Condition	OTP expired/invalid → False path	400: "Invalid or expired OTP"
WB-AUTH-006	login()	Branch	Valid user & password	Token generated, redirect (200)
WB-AUTH-007	login()	Branch	Wrong password / email	401: "Invalid credentials"
WB-AUTH-008	login()	Branch	Unverified user	403: "Email not verified"

.

2. Token Management

Test ID	Function	Test Type	Scenario	Expected Result
WB-TOKEN-001	token_required()	Statement	Valid token decoded	Access granted
WB-TOKEN-002	token_required()	Branch	Missing token	401: "Token is missing"
WB-TOKEN-003	token_required()	Exception	Expired token	401: "Token expired"
WB-TOKEN-004	token_required()	Exception	Invalid format	401: "Token invalid"

3. Scan Configuration

Test ID	Function	Test Type	Scenario / Input	Expected Result
WB-CONFIG-001	configure_scan()	Statement	Valid TCP Connect config	Config parsed correctly
WB-CONFIG-002	configure_scan()	Boundary	Port = 1, 65535	Valid range accepted
WB-CONFIG-003	configure_scan()	Exception	Port > 65535 / invalid	Raises ValueError
WB-CONFIG-004	configure_scan()	Branch	Missing target IP	Raises ValueError
WB-CONFIG-005	configure_scan()	Branch	Unsupported scan type	Raises ValueError
WB-CONFIG-006	configure_scan()	Branch	For idle scan, missing zombie IP	Raises ValueError

TCP SYN Scan

Configure and execute scan

Target IP Address

172.522.2.30

Port Range

1

Start Scan

Invalid target IP address format (must be IPv4 or IPv6)

TCP SYN Scan
Configure and execute scan

Target IP Address
172.25.23.109

Port Range
123534

Start Scan

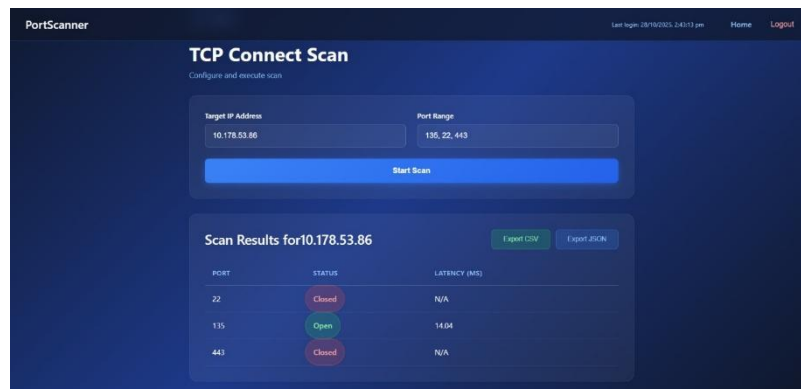Invalid port number: 123534

4. Scanning Functions

Test ID	Function	Test Type	Case	Expected Result
WB-SCAN-001	connect_scan()	Statement	Port open	status = open
WB-SCAN-002	connect_scan()	Branch	Port closed → exception	status = closed
WB-SCAN-003	syn_scan()	Exception	Run without root	PermissionError
WB-SCAN-004	udp_scan()	Branch	ICMP port unreachable	status = closed
WB-SCAN-005	idle_scan()	Statement	Zombie IP check	Correct IPID behavior

5. Input Validation

Test ID	Function	Test Type	Input	Expected Result
WB-VAL-001	validate_ip_address()	Statement	Valid IP	True
WB-VAL-002	validate_ip_address()	Branch	Invalid IP / octet > 255	False
WB-VAL-003	parse_ports()	Boundary	1–65535	Valid
WB-VAL-004	parse_ports()	Boundary	0 / 70000	Invalid

6. Database Operations

Test ID	Function	Test Type	Condition / Input	Expected Result
WB-DB-001	add_user()	Statement	New user	User inserted, OTP generated
WB-DB-002	add_user()	Branch	Duplicate email	Returns None
WB-DB-003	verify_user_otp()	Path	OTP valid → True path	User verified
WB-DB-004	verify_user_otp()	Path	OTP expired → False	No update
WB-DB-005	update_last_login()	Statement	Valid user ID	Timestamp updated

7. Frontend & Integration Coverage

Test ID	Component	Type	Scenario	Expected Result
WB-FE-001	RegisterPage.jsx	Unit	Form validation	Errors shown for empty inputs
WB-FE-002	LoginPage.jsx	Unit	Valid login → API call	Token stored, redirected
WB-FE-003	ProtectedRoute.jsx	Conditional	Authenticated/u nauthenticated	Redirect logic verified
WB-FE-004	ScanPage.jsx	Integration	Valid scan form → API call	Results rendered

8. Security Coverage

Test ID	Module	Scenario	Expected Result
WB-SEC-002	token_required()	Token tampering	Rejected (401)
WB-SEC-003	models.py	Password hashing check	bcrypt hash stored