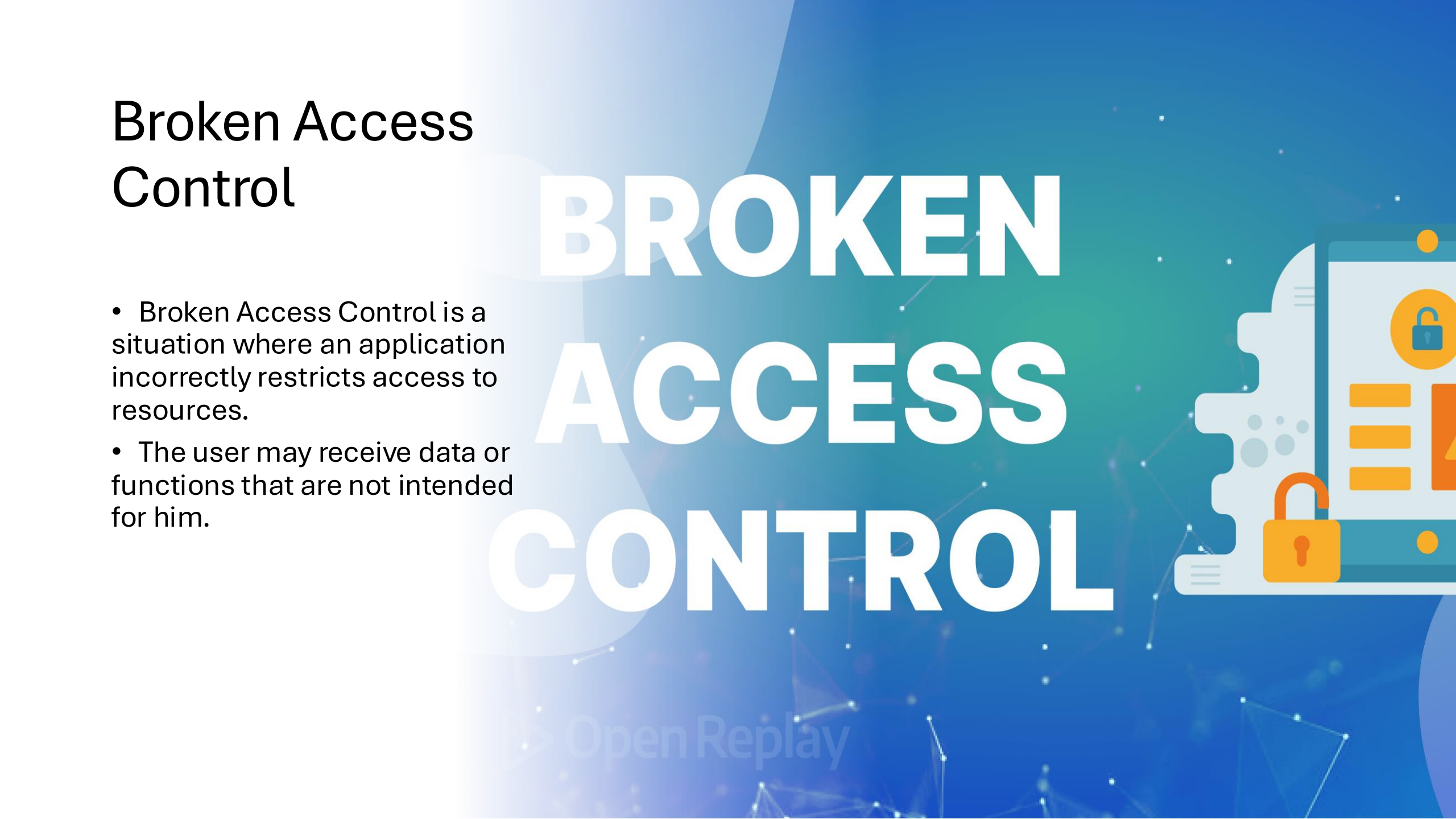
Web Security: Broken Access Control & Security Misconfiguration

Atai Toktosunov

Broken Access Control

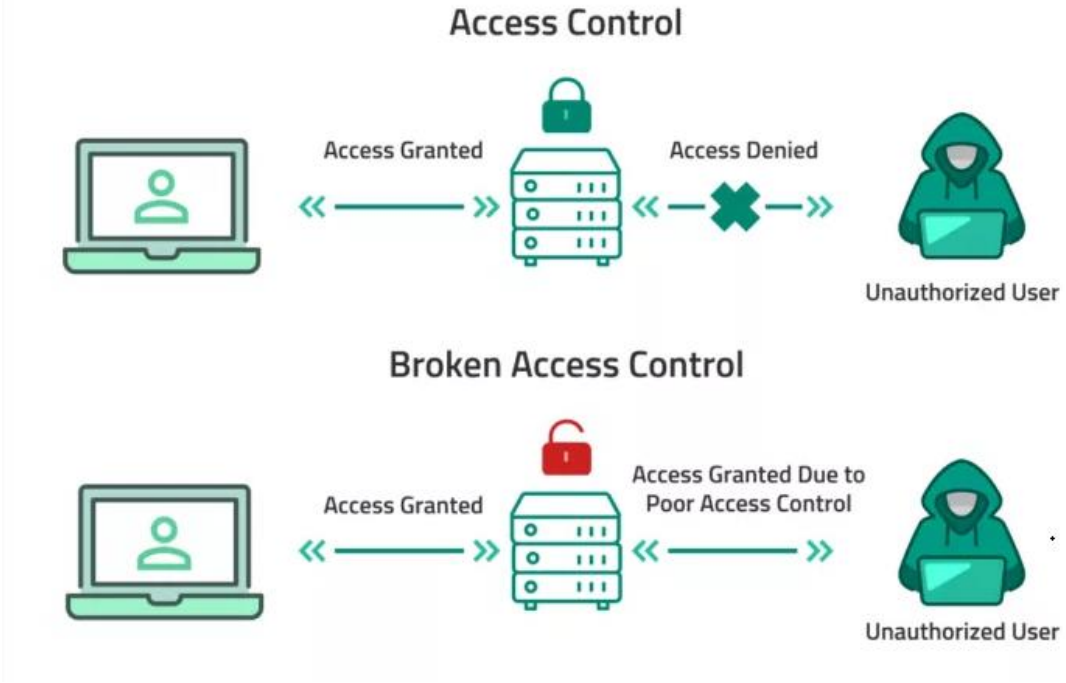
- Broken Access Control is a situation where an application incorrectly restricts access to resources.
- The user may receive data or functions that are not intended for him.



How Hackers Exploit It

Examples of attack:

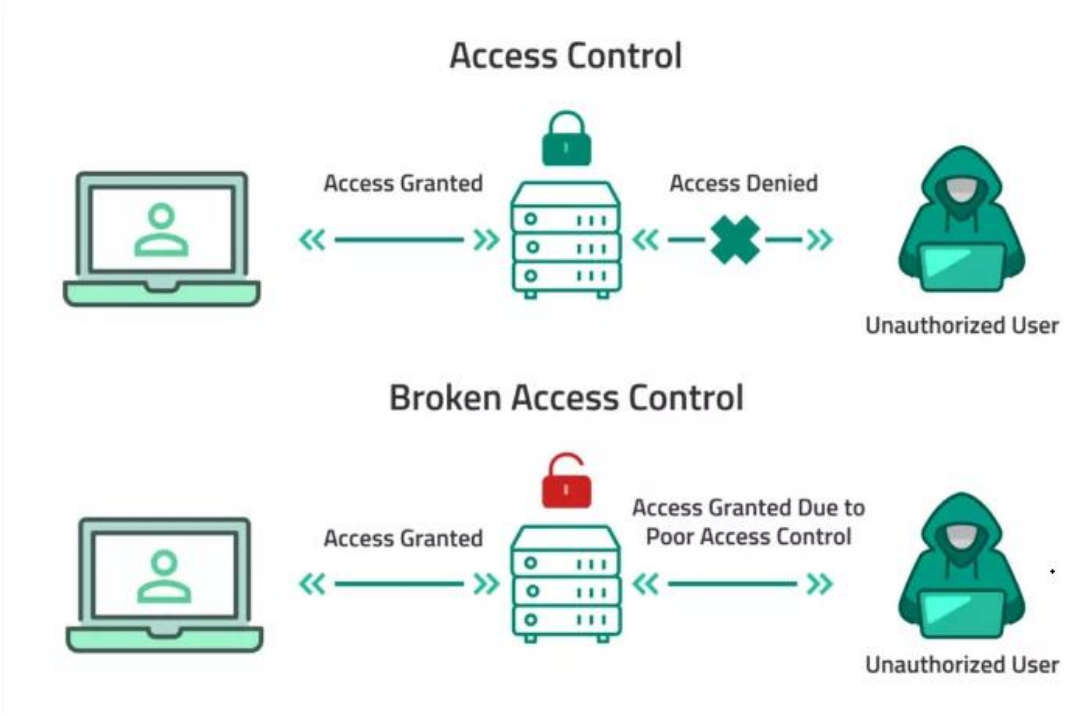
- Change the ID in the URL: /user/101 → user/102
- They send requests via DevTools with the admin role
- They receive files directly via a direct link
- Perform actions that should only be for privileged users.



How to Prevent Broken Access Control

Prevention:

- Checking all rights on the server, not in the browser
- Clear authorization rules (RBAC, roles, permissions)
- Do not trust user data (ID, role, email in the request)
- Restricting access to API routes
- Regular testing of access scenarios



Security Misconfiguration

Definition:

Security Misconfiguration is incorrect server, framework, or database settings.

Examples:

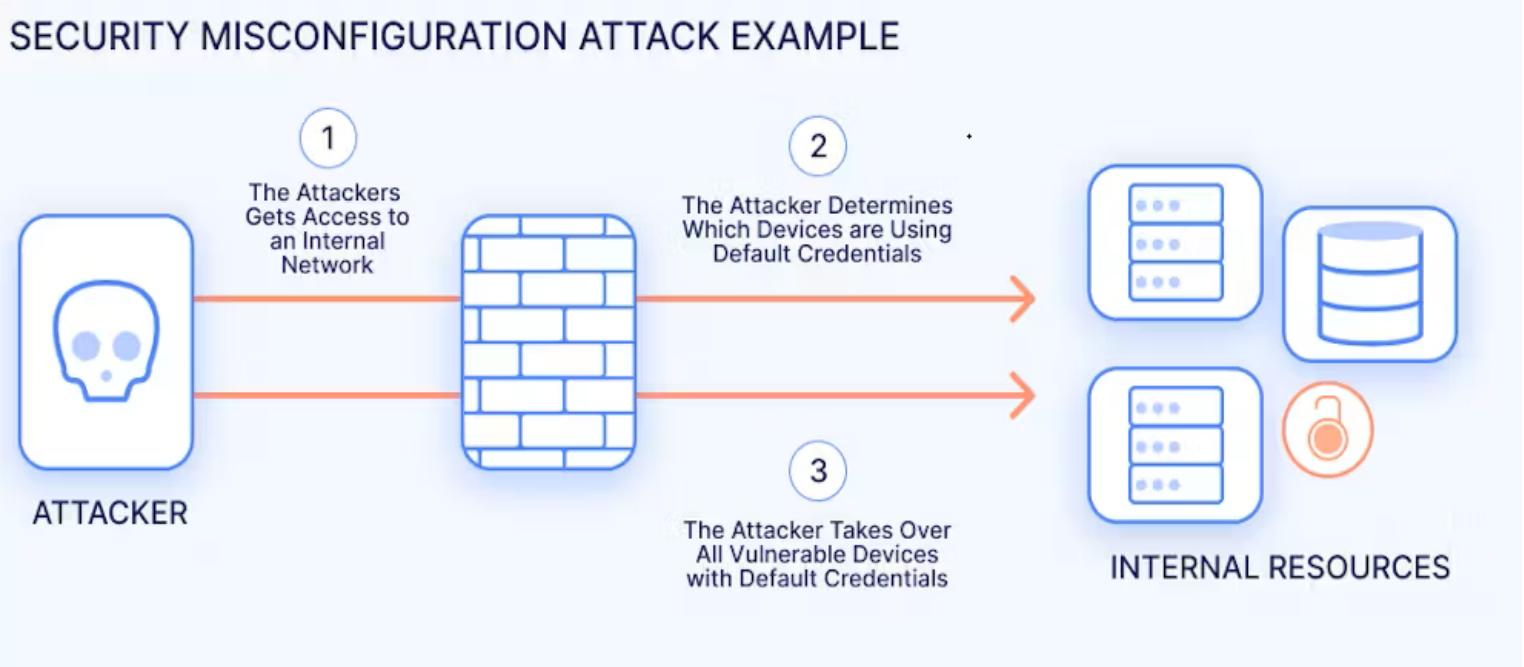
- Debug mode enabled in production
- Unchanged default logins and passwords
- Open admin panels
- Public files and folders that should be closed
- Error messages that are too detailed

curity Misconfiguration

How Hackers Exploit Misconfigurations

Examples:

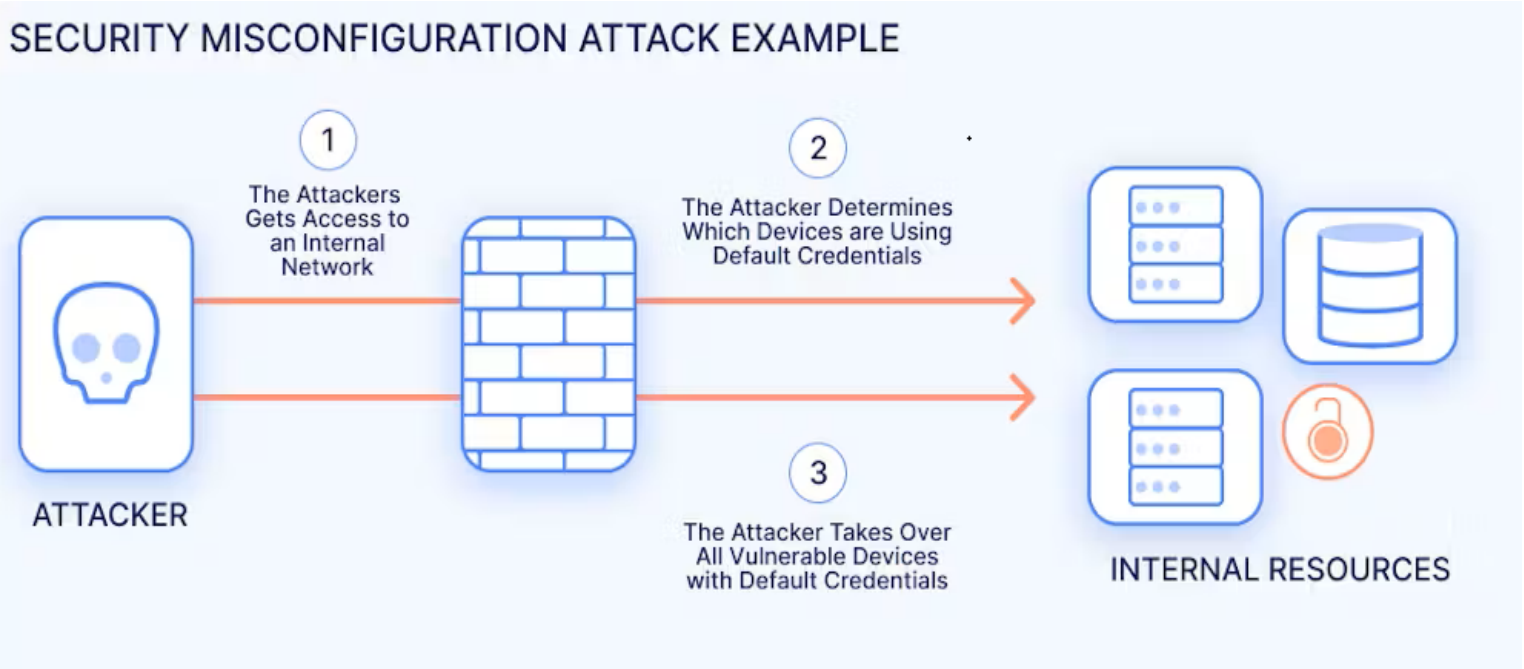
- Through debug panels, they receive a stack trace and secret information.
- They find open MongoDB databases without a password
- They use automatic scanners to find /admin, /phpinfo, /swagger
- Log in to accounts with default passwords: admin/admin

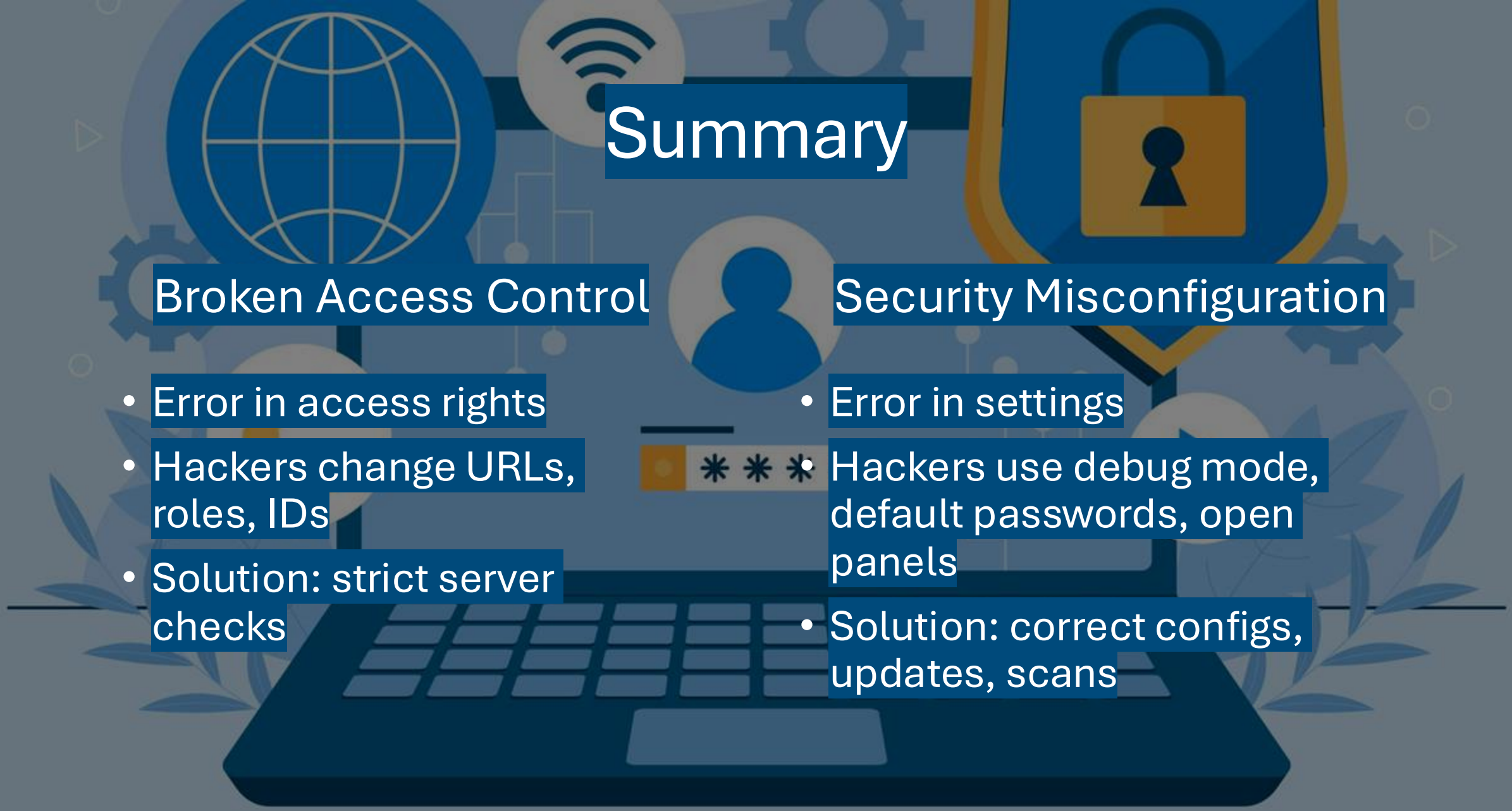


How to Prevent Security Misconfiguration

Prevention:

- Disable debug mode
- Delete test files, temporary APIs, old endpoints
- Change default logins/passwords
- Restrict access to the admin area
- Regularly update the server, packages, and frameworks
- Make automatic security scans (for example, OWASP ZAP)





Summary

Broken Access Control

- Error in access rights
- Hackers change URLs, roles, IDs
- Solution: strict server checks

Security Misconfiguration

- Error in settings
- Hackers use debug mode, default passwords, open panels
- Solution: correct configs, updates, scans