Checklist

Recon

- □ Footprinting
  - □ Nmap
  - □ Evilscan
  - □ Rustscan
  - □ Telnet/Netcat
  - □ Banner Grabbing
  - □ NSE NMAP SCRIPT
- □ Cari informasi sensitif
- □ Cari public exploit
  - □ https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=
  - □ https://packetstormsecurity.com/
  - □ https://www.exploit-db.com/
  - □ https://github.com/
  - □ `"CVE" "keyword"`
- □ Lihat semua protokol
  - □ Cari cara komunikasi dengan protokolnya
    - □ Apa yang biasanya dilakukan orang
      - □ cari di github
      - □ cari di wiki
      - □ cari di manual page
      - □ cari di Top 5, dan semacam tentang cara komunikasinya
      - □ cari di stackoverflow
      - □ cari di forum forum developer
      - □ cari di pembahasan forum, baca setiap thread orang
  - □ Cari semua kerentanan yang pernah terjadi sama protokol itu
    - □ Layanan yang digunakan sama protokol itu (Dalam suatu server)
  - □ Ngertiin konsep dari protokol itu
  - □ Baca tentang cara konfignya
  - □ Cobain di lokal buat layanan dan cara konfignya gimana
  - □ Cari backupan
  - □ Cari notes
  - □ Googling setiap response
  - □ Googling setiap error
  - □ Fokus ke error handling
- □ Phising Scenario, imap/smtp.
- □ Kalo ngerasa ga bisa diapa-apain, skip.

Bypassing WAF

- Origin IP
  - bgptools
  - ipinfo
  - ASN
  - bgp.he.net
  - dnsrecon
  - A
  - NS
  - AAAA
  - subnets/CIDR
- Unicode (whitespace)
- `%0A`
- `%0D`
- `%0C`
- `%0B`

HTTP/HTTPS

- □ Whatweb
- □ Cewl
- □ Nikto
- □ Cari informasi sensitif
- □ Cari error handling
- □ Cari cloud storage
- □ Periksa `.git`.
- □ Backup files:
  - □ .bak
  - □ .tgz
  - □ .tar.xz
  - □ .tar.gz
  - □ .tar
  - □ .zip
  - □ .rar
  - □ .7z
  - □ .txt
  - □ .bkp
  - □ .bp
  - □ .save
  - □ .docx
  - □ .old

  - □ .baka
  - □ .bk
  - □ .backup
  - □ https://en.wikipedia.org/wiki/List_of_archive_formats
  - □ https://fileinfo.com/filetypes/backup
- □ Perhatikan teknologi yang digunakan:
  - □ Header response
  - □ Webserver
  - □ CMS
  - □ Bahasa Pemrograman
  - □ Library
  - □ Meta tag
  - □ Comment tag
  - □ Jenis Cookie
  - □ File Javascript
- □ Directory Fuzzing:
  - □ Feroxbuster
  - □ Dirsearch
- □ TLS/SSL
  - □ sslscan2
- □ Kalo ada subdomain:
  - □ Periksa tcp/53 atau DNS Record:
    - □ Nameserver
    - □ CNAME
    - □ TXT
    - □ bind address
    - □ A
    - □ MX
    - □ NS
  - □ Tools
    - □ dnsrecon
    - □ dnsenum
    - □ dig
    - □ nslookup
- □ Periksa Virtual Host
  - □ wfuzz
  - □ ffuf
- □ Cobain semua fitur aplikasi webnya
- □ Perhatiin WSTG
  - □ Authentication
    - □ Default Credentials
      - □ admin:admin

        - □ root:root
        - □ password:password
        - □ tomcat:tomcat
        - □ manager:manager
        - □ user:user
        - □ `<name>:<name>`
        - □ https://github.com/danielmiessler/SecLists/blob/master/Passwords/Default-Credentials/default-passwords.csv
        - □ https://datarecovery.com/rd/default-passwords/
        - □ https://www.thehacker.recipes/web/config/default-credentials
    - □ Bruteforce
- □ Configuration and Deployment Management
    - □ Test Network Infrastructure Configuration
        - □ Known Server Vulnerabilities
            - □ CVE Public Exploit
            - □ https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=
        - □ Administrative Tools
            - □ WebDAV
            - □ NFS
            - □ CIFS
            - □ FTP
            - □ IIS Server
            - □ Apache
            - □ Nginx
            - □ Express
            - □ Node
            - □ RPC
            - □ SMB
            - □ SSH
    - □ Test Application Platform Configuration
        - □ Sample and Known Files and Directories
        - □ Comment Review
        - □ System Configuration
        - □ Configuration Review
        - □ Logging
        - □ Sensitive Information in Logs
        - □ Log Review
        - □ Log Access Control
        - □ Log Storage
        - □ Log Location
        - □ Log Rotation

- □ File Extensions Handling for Sensitive Information
    - □ .config
    - □ .asa
    - □ .inc
    - □ .zip
    - □ .tar
    - □ .gz
    - □ .tgz
    - □ .rar
    - □ .java
    - □ .txt
    - □ .pdf
    - □ .docx
    - □ .rtf
    - □ .xlsx
    - □ .xls
    - □ .ppt
    - □ .pptx
    - □ .bak
    - □ .old
    - □ .old.extension
    - □ .extension.bak
    - □ .extension.old
- □ HTTP Methods & Headers
    - □ Discover the Supported Methods
        - □ OPTIONS
        - □ TRACE
        - □ DELETE
        - □ PUT
        - □ CONNECT
        - □ PATCH
    - □ Discover HTTP Headers
        - □ Host Header Injection
        - □ Custom Headers
            - □ X-Access-Token
            - □ X-Token
            - □ `X-<Name>`
            - □ Any Custom Header Built-In.
- □ HTTS
- □ Cloud Storage
    - □ S3 Bucket
        - □ aws-cli

    - □ CSP
        - □ https://csp-evaluator.withgoogle.com/
- □ Cari cara buat bypass authentication scheme
    - □ error handling
    - □ kerentanan lain
        - □ LFI
        - □ XXE (SSRF file:///, gopher:///, ftp:///)
        - □ XSS (tergantung skenario)
            - □ XSS > CSRF
            - □ XSS > Steal cookie
                - □ Account takeover
            - □ XSS > SSRF
    - □ Cek fitur password change / reset
        - □ Account takeover
        - □ Generated Token Algorithm
        - □ Cryptography (CryptoJS) (React JS biasanya sering)
        - □ Email Flooding Attack
        - □ No Rate Limit
    - □ Cek fitur ganti email
        - □ Account takeover
        - □ Email Flooding Attack
        - □ No Rate Limit
- □ Business Logic
    - □ File Upload
        - □ Unexpected File Types
            - □ Chain from other to view the file (unexpected).
            - □ For example:
                - □ .txt upload (webshell)
                - □ there's a feature that able to view the .txt
                - □ chain it to .txt file to render the .txt (may able to RCE).
        - □ .svg (Self-XSS) to Account Takeover (steal cookie / token)
        - □ malicious file
            - □ .phar
            - □ .phtml
            - □ .pht
            - □ .aspx
            - □ .asp
            - □ .jsp
            - □ .war
            - □ .exe
            - □ .pdf (xss)
    - □ Coupon Code

  - □ VA Account Number Fuzzing
  - □ Process Timing
    - □ No Rate Limit
  - □ Integrity Checks
  - □ Business Logic Data Validation
  - □ Forge Requests (Forcing Disabled Features)
  - □ Any Business Process Included
- □ Error Handling
  - □ Improper Error Handling
  - □ Stack Trace
- □ Client-Side Attack
  - □ DOM XSS
  - □ JS Execution
  - □ HTML Injection
  - □ Client-side URL Redirect
  - □ CSS Injection
  - □ Client-side Resource Manipulation
  - □ CORS
  - □ Cross Site Flashing
  - □ Clickjacking
  - □ Websocket
  - □ Web Messaging
  - □ Browser Storage
    - □ Local Storage
    - □ Session Storage
    - □ Cookie
  - □ Cross Site Script Inclusion
  - □ Reverse Tabnabbing
- □ Input Validation
  - □ XSS
    - □ Stored
    - □ DOM
      - □ Stored DOM XSS
      - □ Reflected DOM XSS
      - □ functions:
        - □ document.write()
        - □ document.writeln()
        - □ document.domain
        - □ element.innerHTML
        - □ element.outerHTML
        - □ element.insertAdjacentHTML
        - □ element.onevent

- [ ] add()
- [ ] after()
- [ ] append()
- [ ] animate()
- [ ] insertAfter()
- [ ] insertBefore()
- [ ] before()
- [ ] html()
- [ ] prepend()
- [ ] replaceAll()
- [ ] replaceWith()
- [ ] wrap()
- [ ] wrapInner()
- [ ] wrapAll()
- [ ] has()
- [ ] constructor()
- [ ] init()
- [ ] index()
- [ ] jQuery.parseHTML()
- [ ] $.parseHTML()

- [ ] Reflected

- [ ] Parameter
  - [ ] Parameter Pollution
    - [ ] `?test=a&test=a` will get 2 outputs.
  - [ ] Arbitrary Parameter Input
    - [ ] Open Redirect
    - [ ] Forcing Parameter Value Input Validation
      - [ ] `id=1` into `id=testing` = from `{ "id": 1 }` to `{ "id": "testing" }`
- [ ] SQL Injection
  - [ ] file write
  - [ ] Second Order Request
  - [ ] authorized_keys write
  - [ ] file read
    - [ ] /proc/self
      - [ ] cmdline
      - [ ] environ
      - [ ] status
      - [ ] stat
      - [ ] cwd/
        - [ ] filename.extension
    - [ ] /etc
      - [ ] passwd

      - □ groups
      - □ shells
      - □ apache config
      - □ nginx config
      - □ webserver config
      - □ ssh/sshd_config
      - □ systemd/systemd/sshd.service
  - □ upload shell
  - □ UDF
    - □ postgres
    - □ mssql
    - □ mysql
  - □ blind boolean-based
  - □ error-based
  - □ union-based
  - □ blind time-based
  - □ stacked queries
- □ XML Injection
- □ LDAP Injection
- □ XPATH Injection`
- □ IMAP and SMTP Injection
- □ XXE
  - □ php wrapper
  - □ `expect://`
  - □ ssrf
  - □ blind oob
  - □ blind dtd
- □ SSTI
  - □ cek waf
  - □ cek blacklist word
  - □ enum setiap objeknya
  - □ pake Fenjing
    - □ https://github.com/Marven11/Fenjing
- □ SSRF
  - □ leak local port
  - □ leak pake responder
  - □ leak data/creds pake python server
  - □ leak data/creds pake ftp
- □ Open Redirect
- □ Command Injection
  - □ payloadallthethings is nice
  - □ `%0A`

    - □ Unicode
      - □ Line Feed `\n`
      - □ Tab `\t`
      - □ Return `\r`
      - □ Alert `\a`
      - □ Backspace `\b`
      - □ Whitespace
      - □ https://www.compart.com/en/unicode/
    - □ commix
    - □ hacktricks command injection
  - □ HTTP Smuggling
    - □ CL.TE
    - □ TE.CL
      - □ Account Takeover
    - □ TE.TE
  - □ Local File Inclusion
    - □ /etc/stuff
    - □ /proc/self
      - □ environ
      - □ status
      - □ mounts
      - □ etc etc
    - □ /proc/cwd
    - □ Service Log /var/log
    - □ Service Error Log /var/log
    - □ If PHP, php chain gadget
      - □ https://github.com/synacktiv/php_filter_chain_generator/blob/main/php_filter_chain_generator.py
      - □ = --data-urlencode '0='
    - □ Directory Traversal
      - □ ..//
      - □ ....//
      - □ ..../
      - □ .../
      - □ ..///
      - □ ...//
- □ PHP Type Juggling
  - □ `0e` Loose Comparison `!=` and `==`
  - □ `0e` Strict Comparison `===` or `!==`
- □ Authorization
  - □ Directory Traversal

    - □ Local File Inclusion
    - □ BAC (Bypass Authorization Scheme) or (Broken Access Control)
    - □ Privilege Escalation (Client Side, JavaScript)
    - □ Privilge Escalation (Server-side)
    - □ IDOR
        - □ GET
        - □ POST
        - □ PUT
        - □ DELETE
        - □ Depends On How Business Proceeds
    - □ OAuth
        - □ Authorization Server Weakness
        - □ Authorization Client Weakness
        - □ XSS
        - □ Token In URL
- □ Session Management
    - □ Bentuk cookie
        - □ PHPSESSION
        - □ Flask Sign
            - □ flask-unsign
        - □ JWT
            - □ jwt.io
        - □ Serialization
            - □ Java Deserialization
                - □ ysoserial
            - □ PHP Deserialization
                - □ phpggc
            - □ ViewState Deserialization
                - □ ysoserial.net
            - □ JSESSION
    - □ Kerentanan session
    - □ Apa yang bisa dimanfaatkan dari session
        - □ ke akun lain
        - □ buat akses API
        - □ buat akses halaman
        - □ buat akses aset
    - □ CSRF
    - □ Session
        - □ Hijacking
        - □ Fixation
        - □ Puzzling
    - □ Logout Functionality

- [ ] Identity Management
    - [ ] Perhatiin definisi rolenya
    - [ ] Perhatiin proses registrasi dan login
    - [ ] Pembuatan akun tanpa proses registrasi yang valid pada aplikasi
    - [ ] Username enumeration
- [ ] API Testing
    - [ ] GraphQL
    - [ ] Express
    - [ ] gRPC
    - [ ] JSON-RPC
    - [ ] SOAP
    - [ ] Apache Thrift
    - [ ] XML-RPC

Mobile (taught by akewcrafts)

- Check anti frida hook
    - Functions
    - Methods
    - Obfuscation Method
- Check anti tampering
    - Functions
    - Methods
    - Obfuscation Method
- Check anti frida detection
    - Functions
    - Methods
    - Obfuscation Method
- Check root detection
    - Functions
    - Methods
    - Obfuscation Method
- Check data handling storage
    - sqlite `.db`
    - internal storage
        - openFileInput()
        - openFileOutput()
    - sharedPreferences
    - Cloud Storage
- Check SSL Pinning
    - Functions

    - Methods
    - Obfuscation Method
- Check RASP (Runtime application self-protection)
    - is the RASP custom?
    - is the RASP internet product in the wild?
    - is the RASP open source?
    - is the RASP famous?
- Maybe there's
    - anti debugging?
    - anti virtualization?
    - mutex implementation?
    - any other protection stuff?
- FLUTTER (?!)

Javascript

- □ DOM XSS
- □ Javascript Files
    - □ Custom Headers
    - □ Custom Cookies
    - □ Browser Storage
        - □ Session Storage
        - □ Local Storage
    - □ POST, PUT, GET, DELETE, PATCH Endpoints
    - □ Custom Encryption
- □ Node JS / Express JS
    - □ Prototype Pollution
        - □ Check for spawned process for RCE `[object Object]` gadget
            - □ child_process or other similar stuff
        - □ If not, check all the calling conventions for `[object Object]`
            - □ Bypass the condition with:
                - □ `__proto__`
                - □ `constructor.prototype`
                - □ adding whitespace
                - □ adding null byte
                - □ adding unicode
                - □ adding double urlencode

Python

- □ Format String

    - □ `{people_obj.__init__.__globals__[CONFIG][KEY]}`
- □ eval()
    - □ `__import__('os').system('id')`
- □ YAML Deserialization
    - □ https://book.hacktricks.xyz/pentesting-web/deserialization/python-yaml-deserialization
- □ Pickle Deserialization

```
import pickle, os, base64
class P(object):
    def __reduce__(self):
        return (os.system,("/bin/bash -c '/bin/id > /tmp/pwned.txt'",))
print(base64.b64encode(pickle.dumps(P())))
```

- □ Werkzeug Console Pin Bypass
    - □ https://github.com/wdahlenburg/werkzeug-debug-console-bypass/blob/main/README.md
    - □ google it urself
- □ Sandbox escape
    - □ https://book.hacktricks.xyz/generic-methodologies-and-resources/python/bypass-python-sandboxes
- □ Prototype Pollution
    - □ https://book.hacktricks.xyz/generic-methodologies-and-resources/python/class-pollution-pythons-prototype-pollution
- □ Pyscript

```
<py-script>
        with open('/lib/python3.10/site-packages/_pyodide/_base.py', 'r') as fin:
        out = fin.read()
        print(out)
</py-script>
```

Java

- □ https://github.com/KINGSABRI/godofwar
- □ Java RMI
    - □ https://github.com/qtc-de/remote-method-guesser
    - □ ysoserial

PHP

- □ Magic Hashes

- □ Magic Bytes
- □ Functions
  - □ `preg_replace()` command exec
  - □ `exec()`
  - □ `system()`
  - □ `shell_exec()`
  - □ `passthru()`
  - □ using ``
  - □ using `fread(popen("/bin/id", "r"), 4096)`
  - □ using `proc_close(proc_open("id",array(),$peler));`
  - □ using `preg_replace('/.*/e', 'system("whoami");', '');`
  - □ using `pcntl_exec("/bin/id");`
  - □ using `dl()`
  - □ `file_put_contents('/tmp/peler.sh', base64_decode('IyEvYmluL3NoCi9yZWFkZmxhZyA+IC90bXAvZmxhZy50eHQKCg==')); chmod('/tmp/peler.sh', 0777); mail('', '', '', '', '-H \"exec /tmp/peler.sh\"'); echo file_get_contents('/tmp/flag.txt');`
  - □ `eval()`
  - □ `assert()`
  - □ `$_GET['func_name']($_GET['argument']);`
  - □ `require_once()`
  - □ `require()`
  - □ `include_once()`
  - □ `include()`
  - □ `file_gets_content()`
  - □ `file_put_content()`
  - □ https://github.com/Medicean/as_bypass_php_disable_functions
  - □ https://github.com/giovannichhatta/disable-functions-bypass
  - □ Windows
    - □ https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/php-tricks-esp/php-useful-functions-disable_functions-open_basedir-bypass/disable_functions-bypass-php-less-than-5.2.9-on-windows