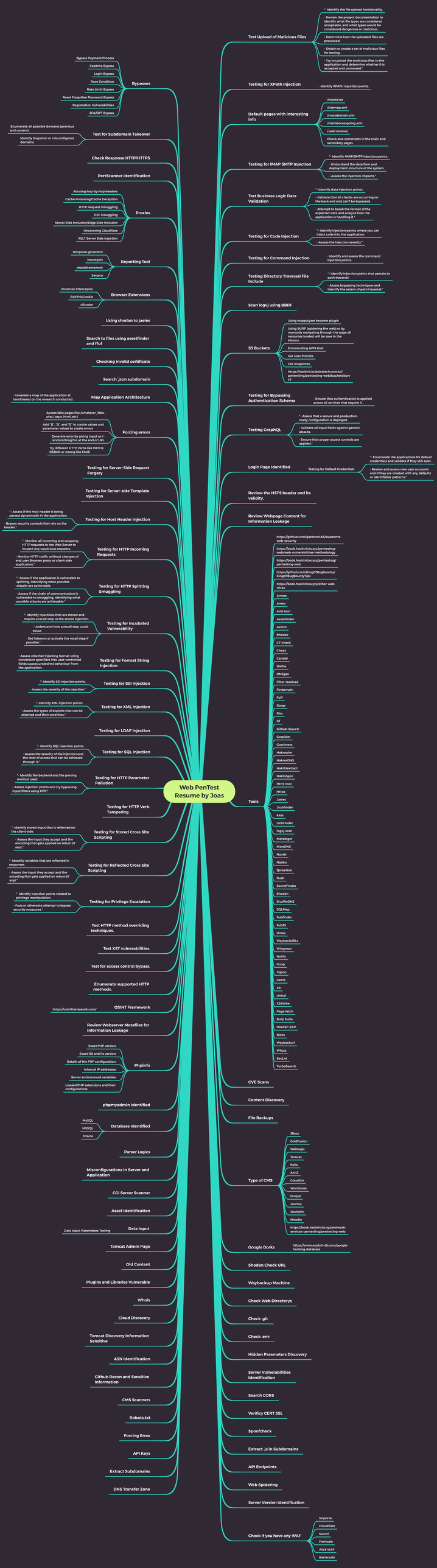
Web PenTest
Resume by Joas
Test Upload of Malicious Files
*- Identify the file upload functionality.
- Review the project documentation to determine what types of files are considered acceptable, and what types would be considered dangerous or malicious.
- Determine how the uploaded files are processed.
- Obtain or create a set of malicious files for testing.
- Try to upload the malicious files to the application and determine whether it is accepted and processed.*
Testing for XPath Injection
- Identify XPATH injection points.
Default pages with interesting info
/robots.txt
/sitemap.xml
/crossdomain.xml
/clientaccesspolicy.xml
/.well-known/
Check also comments in the main and secondary pages.
Testing for IMAP SMTP Injection
*- Identify IMAP/SMTP injection points.
- Understand the data flow and deployment structure of the system.
- Assess the injection impacts.*
Test Business Logic Data Validation
*- Identify data injection points.
- Validate that all checks are occurring on the back end and can't be bypassed.
- Attempt to break the format of the expected data and analyze how the application is handling it.*
Testing for Code Injection
*- Identify injection points where you can inject code into the application.
- Assess the injection severity.*
Testing for Command Injection
- Identify and assess the command injection points.
Testing Directory Traversal File Include
*- Identify injection points that pertain to path traversal.
- Assess bypassing techniques and identify the extent of path traversal.*
Scan log4j using BBRF.
S3 Buckets
Using wappalyzer browser plugin
Using BURP (spidering the web) or by manually navigating through the page all resources loaded will be save in the History.
Enumerating AWS User
Get User Policies
Get Snapshots
https://hacktricks.boitatech.com.br/pentesting/pentesting-web/buckets/aws-s3
Testing for Bypassing Authentication Schema
- Ensure that authentication is applied across all services that require it.
Testing GraphQL
*- Assess that a secure and production-ready configuration is deployed.
- Validate all input fields against generic attacks.
- Ensure that proper access controls are applied.*
Login Page Identified
Testing for Default Credentials
*- Enumerate the applications for default credentials and validate if they still exist.
- Review and assess new user accounts and if they are created with any defaults or identifiable patterns.*
Review the HSTS header and its validity.
Review Webpage Content for Information Leakage
Tools
https://github.com/gazbnm456/awesome-web-security
https://book.hacktricks.xyz/pentesting-web/web-vulnerabilities-methodology
https://book.hacktricks.xyz/pentesting/pentesting-web
https://github.com/KingOfBugbounty/KingOfBugBountyTips
https://book.hacktricks.xyz/other-web-tricks
Amass
Anew
Anti-burl
Assetfinder
Axiom
Bhedak
CF-check
Chaos
Ceriddi
Dalfox
DNSgen
Filter-resolved
Findomain
Fuff
Gargs
Gau
Gf
Github-Search
Gospider
Gowitness
Hakrawler
HakrevDNS
Haktldextract
Haksitegen
Html-tool
Httpx
Jaales
Jsubfinder
Kxss
LinkFinder
log4j-scan
Metabigor
MassDNS
Nuclei
Naabu
Qsreplace
Rush
SecretFinder
Shodan
ShuffleDNS
SQLMap
Subfinder
Sub2S
Unew
WaybackURLs
Wingman
Notify
Goop
Trojon
GetJS
X8
Linkurl
XSStrike
Page-fetch
Burp Suite
OWASP-ZAP
Nikto
Waybackurl
Wfuzz
SecList
TurboSearch
CVE Scans
Content Discovery
File Backups
Type of CMS
JBoss
ColdFusion
Weblogic
Tomcat
Railo
Axis2
Glassfish
Wordpress
Drupal
Joomla
vbulletin
Moodle
https://book.hacktricks.xyz/network-services-pentesting/pentesting-web
Google Dorks
https://www.exploit-db.com/google-hacking-database
Shodan Check URL
Waybackup Machine
Check Web Directorys
Check .git
Check .env
Hidden Parameters Discovery
Server Vulnerabilities Identificaiton
Search CORS
Verifiy CERT SSL
Spoofcheck
Extract .js in Subdomains
API Endpoints
Web Spidering
Server Version Identification
Check if you have any WAF
Imperva
Cloudflare
Sucuri
Fortiweb
AWS WAF
Barracuda
Bypasses
Bypass Payment Process
Captcha Bypass
Login Bypass
Race Condition
Rate Limit Bypass
Reset Forgotten Password Bypass
Registration Vulnerabilities
2FA/OPT Bypass
Test for Subdomain Takeover
Enumerate all possible domains (previous and current).
Identify forgotten or misconfigured domains.
Check Response HTTP/HTTPS
PortScanner Identification
Proxies
Abusing hop-by hop headers
Cache Poisoning/Cache Deception
HTTP Request Smuggling
H2C Smuggling
Server Side Inclusion/Edge Side Inclusion
Uncovering Cloudflare
XSLT Server Side Injection
Reporting Tool
template-generator
bountyplz
dradisframework
Serpico
Browser Extensions
Postman Interceptor
EditThisCookie
d3coder
Using shodan to jaeles
Search to files using assetfinder and ffuf
Checking invalid certificate
Search .json subdomain
Map Application Architecture
- Generate a map of the application at hand based on the research conducted.
Forcing errors
Access fake pages like /whatever_fake.php (.aspx,.html,.etc)
Add "[]", "]]", and "[[" in cookie values and parameter values to create errors
Generate error by giving input as /~randomthing/%s at the end of URL
Try different HTTP Verbs like PATCH, DEBUG or wrong like FAKE
Testing for Server-Side Request Forgery
Testing for Server-side Template Injection
Testing for Host Header Injection
*- Assess if the Host header is being parsed dynamically in the application.
- Bypass security controls that rely on the header.*
Testing for HTTP Incoming Requests
*- Monitor all incoming and outgoing HTTP requests to the Web Server to inspect any suspicious requests.
- Monitor HTTP traffic without changes of end user Browser proxy or client side application.*
Testing for HTTP Splitting Smuggling
*- Assess if the application is vulnerable to splitting, identifying what possible attacks are achievable.
- Assess if the chain of communication is vulnerable to smuggling, identifying what possible attacks are achievable.*
Testing for Incubated Vulnerability
*- Identify injections that are stored and require a recall step to the stored injection.
- Understand how a recall step could occur.
- Set listeners or activate the recall step if possible.*
Testing for Format String Injection
- Assess whether injecting format string conversion specifiers into user-controlled fields causes undesired behaviour from the application.
Testing for SSI Injection
*- Identify SSI injection points.
- Assess the severity of the injection.*
Testing for XML Injection
*- Identify XML injection points.
- Assess the types of exploits that can be attained and their severities.*
Testing for LDAP Injection
Testing for SQL Injection
*- Identify SQL injection points.
- Assess the severity of the injection and the level of access that can be achieved through it.*
Testing for HTTP Parameter Pollution
*- Identify the backend and the parsing method used.
- Assess injection points and try bypassing input filters using HPP.*
Testing for HTTP Verb Tampering
Testing for Stored Cross Site Scripting
*- Identify stored input that is reflected on the client side.
- Assess the input they accept and the encoding that gets applied on return (if any).*
Testing for Reflected Cross Site Scripting
*- Identify variables that are reflected in responses.
- Assess the input they accept and the encoding that gets applied on return (if any).*
Testing for Privilege Escalation
*- Identify injection points related to privilege manipulation.
- Fuzz or otherwise attempt to bypass security measures.*
Test HTTP method overriding techniques.
Test XST vulnerabilities.
Test for access control bypass.
Enumerate supported HTTP methods.
OSINT Framework
https://osintframework.com/
Review Webserver Metafiles for Information Leakage
Phpinfo
Exact PHP version.
Exact OS and its version.
Details of the PHP configuration.
Internal IP addresses.
Server environment variables.
Loaded PHP extensions and their configurations.
phpmyadmin Identified
Database Identified
MySQL
MSSQL
Oracle
Parser Logics
Misconfigurations in Server and Application
CGI Server Scanner
Asset Identification
Data Input
Data Input Parameters Testing
Tomcat Admin Page
Old Content
Plugins and Libraries Vulnerable
Whois
Cloud Discovery
Tomcat Discovery Information Sensitive
ASN Identification
Github Recon and Sensitive Information
CMS Scanners
Robots.txt
Forcing Erros
API Keys
Extract Subdomains
DNS Transfer Zone