SECGURU – Web Application Cheat Sheet

Reconnaissance

- Application & Version
- Web Components
- Domain Structure
- SSL Support? If yes, then what version & ciphers.
- Complete check of information returned in error messages
- Guess application logic through errors codes and messages.
- Gain database information
- Any Critical Data passed over non-ssl?
- Chances of Web Application use via public kiosk? What information is available from cache/temp folders?
- Valuable Phishing Target?
- Provision for Auto-Logon?

Parameter Checklist

- URL request
- URL encoding
- Query string
- Header
- Cookie
  - □ Expire Time
  - □ Secure
  - □ Persistent
- Form fields
  - □ Type
  - □ Length
  - □ Format
  - □ Range
- Hidden field
- Only Client side validation?
- ‘Tainted’ parameters
- Min/Max lengths
- Concatenate commands

Session Management

- Token protection
- Session Duration
- Idle time Duration
- Guess Session ID format
- Transfer in URL or BODY?
- Is Session Id linked to the IP?
- Session X’fer (sso application)
- Change Referrer tag
- Examine
  - □ Token
  - □ Cookie
  - □ SSID
- Serialized Objects
- Conduct replay attack
- Concurrent Logins
- Separate Personalization and session cookies
- Encrypted Cookies, Marked Secure?
- Using Cache-Control Pragma?

Access Control

- Flaws in access control?
- Check for path transversal
- Determine file permissions
- Direct Access to Conf Files
- Is critical data secured and encrypted?
- Access points
  - □ Regular users
  - □ Admin access
  - □ Any other?
- Ability to brute force at the discovered access points.
- Forced browsing, does application keep a check by tracking request from each user
- No Access to system level resources
- Determine access to content and functions, should match company policies.

Mis-Configuration

- Nikto results
- Nessus results
- Investigate Patch Levels
- Directory listing
- Directory permission
- Detailed Error messages
- Default username/pass
- SSL cert. Configuration
- Debug or configuration Files
- Check Latest vulnerabilities
- Unwanted
  - □ Backup files
  - □ Defaults files
  - □ Services
- Remote admin. Access

Credential Management

- Password storage
- Password change
- User Update section
- Password strength
- Lockout policy
- Login attempts allowed
- Account Mgmt. Policies

Authentication

- Un-Encrypted Auth
- Backend Authentication
- Using Least privilege account
- Any Trust relationships
- Use of Encryption
- Text password in HTML
- Text Password in Config
- Ability to bypass auth with spoofed tokens

OS calls

- Using any interpreter?
- OS service calls (e.g. Sendmail)
- Mirror and search code for all calls to external sources.
- Privileges given to other services and web server.
- Deconstruction of binary codes (if any)

SQL injection

- Using Least privilege account
- Mirror website and search for all input parameters
- Gain database related information
- Detailed Error Messages
- Privileges given to the web server or database
- Access only to stored procedures
- Safe failure in case of exception

XSS

- Which type – stored or reflected
- Check for 404/500 error pages for return information.
- Input validation checks
  - □ Type
  - □ Length
  - □ Format
  - □ Range
- Safe failure in case of exception.