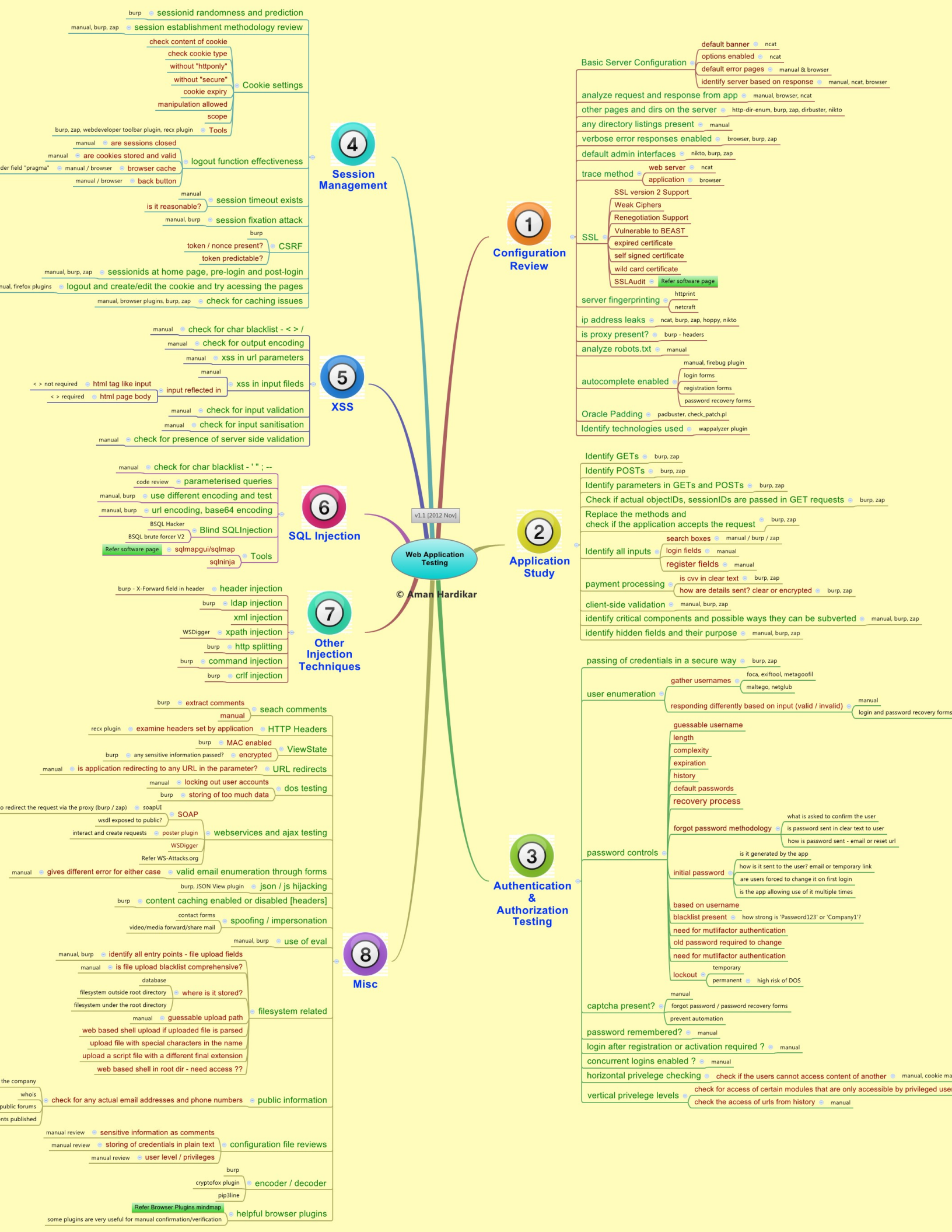
Web Application Testing
v1.1 [2012 Nov]
© Aman Hardikar
1 Configuration Review
Basic Server Configuration
default banner ncat
options enabled ncat
default error pages manual & browser
identify server based on response manual, ncat, browser
analyze request and response from app manual, browser, ncat
other pages and dirs on the server http-dir-enum, burp, zap, dirbuster, nikto
any directory listings present manual
verbose error responses enabled browser, burp, zap
default admin interfaces nikto, burp, zap
trace method web server ncat
application browser
SSL
SSL version 2 Support
Weak Ciphers
Renegotiation Support
Vulnerable to BEAST
expired certificate
self signed certificate
wild card certificate
SSLAudit Refer software page
server fingerprinting httprint
netcraft
ip address leaks ncat, burp, zap, hoppy, nikto
is proxy present? burp - headers
analyze robots.txt manual
autocomplete enabled manual, firebug plugin
login forms
registration forms
password recovery forms
Oracle Padding padbuster, check_patch.pl
Identify technologies used wappalyzer plugin
2 Application Study
Identify GETs burp, zap
Identify POSTs burp, zap
Identify parameters in GETs and POSTs burp, zap
Check if actual objectIDs, sessionIDs are passed in GET requests burp, zap
Replace the methods and check if the application accepts the request burp, zap
Identify all inputs search boxes manual / burp / zap
login fields manual
register fields manual
payment processing is cvv in clear text burp, zap
how are details sent? clear or encrypted burp, zap
client-side validation manual, burp, zap
identify critical components and possible ways they can be subverted manual, burp, zap
identify hidden fields and their purpose manual, burp, zap
3 Authentication & Authorization Testing
passing of credentials in a secure way burp, zap
user enumeration
gather usernames foca, exiftool, metagoofil
maltego, netglub
responding differently based on input (valid / invalid) manual
login and password recovery forms
password controls
guessable username
length
complexity
expiration
history
default passwords
recovery process
forgot password methodology what is asked to confirm the user
is password sent in clear text to user
how is password sent - email or reset url
initial password is it generated by the app
how is it sent to the user? email or temporary link
are users forced to change it on first login
is the app allowing use of it multiple times
based on username
blacklist present how strong is 'Password123' or 'Company1'?
need for mutlifactor authentication
old password required to change
need for mutlifactor authentication
lockout temporary
permanent high risk of DOS
captcha present? manual
forgot password / password recovery forms
prevent automation
password remembered? manual
login after registration or activation required ? manual
concurrent logins enabled ? manual
horizontal privelege checking check if the users cannot access content of another manual, cookie ma
vertical privelege levels check for access of certain modules that are only accessible by privileged use
check the access of urls from history manual
4 Session Management
burp sessionid randomness and prediction
manual, burp, zap session establishment methodology review
Cookie settings
check content of cookie
check cookie type
without "httponly"
without "secure"
cookie expiry
manipulation allowed
scope
burp, zap, webdeveloper toolbar plugin, recx plugin Tools
logout function effectiveness
manual are sessions closed
manual are cookies stored and valid
der field "pragma" manual / browser browser cache
manual / browser back button
manual
is it reasonable? session timeout exists
manual, burp session fixation attack
CSRF
burp
token / nonce present?
token predictable?
manual, burp, zap sessionids at home page, pre-login and post-login
nual, firefox plugins logout and create/edit the cookie and try acessing the pages
manual, browser plugins, burp, zap check for caching issues
5 XSS
manual check for char blacklist - < > /
manual check for output encoding
manual xss in url parameters
xss in input fileds
manual
input reflected in
< > not required html tag like input
< > required html page body
manual check for input validation
manual check for input sanitisation
manual check for presence of server side validation
6 SQL Injection
manual check for char blacklist - ' " ; --
code review parameterised queries
manual, burp use different encoding and test
manual, burp url encoding, base64 encoding
Blind SQLInjection
BSQL Hacker
BSQL brute forcer V2
Tools
sqlmapgui/sqlmap
Refer software page
sqlninja
7 Other Injection Techniques
burp - X-Forward field in header header injection
burp ldap injection
xml injection
WSDigger xpath injection
burp http splitting
burp command injection
burp crlf injection
8 Misc
burp extract comments
manual
seach comments
recx plugin examine headers set by application HTTP Headers
burp MAC enabled
burp any sensitive information passed? encrypted
ViewState
manual is application redirecting to any URL in the parameter? URL redirects
manual locking out user accounts
burp storing of too much data
dos testing
o redirect the request via the proxy (burp / zap) soapUI
wsdl exposed to public?
SOAP
interact and create requests poster plugin
WSDigger
Refer WS-Attacks.org
webservices and ajax testing
manual gives different error for either case valid email enumeration through forms
burp, JSON View plugin json / js hijacking
burp content caching enabled or disabled [headers]
contact forms
video/media forward/share mail
spoofing / impersonation
manual, burp use of eval
manual, burp identify all entry points - file upload fields
manual is file upload blacklist comprehensive?
database
filesystem outside root directory
filesystem under the root directory
where is it stored?
manual guessable upload path
web based shell upload if uploaded file is parsed
upload file with special characters in the name
upload a script file with a different final extension
web based shell in root dir - need access ??
filesystem related
the company
whois
public forums
nts published
check for any actual email addresses and phone numbers public information
manual review sensitive information as comments
manual review storing of credentials in plain text
manual review user level / privileges
configuration file reviews
burp
cryptofox plugin
pip3line
encoder / decoder
Refer Browser Plugins mindmap
some plugins are very useful for manual confirmation/verification
helpful browser plugins