Web Application Penetration Testing Checklist

More than 200 custom testcases

Prepared by: Tushar Verma

- **Recon Phase**
  - [ ] Identify web server, technologies and database
  - [ ] Subsidiary and Acquisition Enumeration
  - [ ] Reverse Lookup
  - [ ] ASN & IP Space Enumeration and Service Enumeration
  - [ ] Google Dorking
  - [ ] Github Recon
  - [ ] Directory Enumeration
  - [ ] IP Range Enumeration
  - [ ] JS Files Analysis
  - [ ] Subdomain Enumeration and Bruteforcing
  - [ ] Subdomain Takeover
  - [ ] Parameter Fuzzing
  - [ ] Port Scanning
  - [ ] Template-Based Scanning(Nuclei)
  - [ ] Wayback History
  - [ ] Broken Link Hijacking
  - [ ] Internet Search Engine Discovery
  - [ ] Misconfigured Cloud Storage
- **Registration Feature Testing**
  - [ ] Check for duplicate registration/Overwrite existing user
  - [ ] Check for weak password policy
  - [ ] Check for reuse existing usernames
  - [ ] Check for insufficient email verification process
  - [ ] Weak registration implementation-Allows disposable email addresses
  - [ ] Weak registration implementation-Over HTTP
  - [ ] Overwrite default web application pages by specially crafted username registrations. ⇒ After registration, does your profile link appears something as www.tushar.com/tushar?

a. If so, enumerate default folders of web application such as /images, /contact, /portfolio

b. Do a registration using the username such as images, contact, portfolio

c. Check if those default folders have been overwritten by your profile link or not."

- **Session Management Testing**
  - [ ] Identify actual session cookie out of bulk cookies in the application
  - [ ] Decode cookies using some standard decoding algorithms such as Base64, hex, URL, etc
  - [ ] Modify cookie.session token value by 1 bit/byte. Then resubmit and do the same for all tokens. Reduce the amount of work you need to perform in order to identify which part of the token is actually being used and which is not
  - [ ] If self-registration is available and you can choose your username, log in with a series of similar usernames containing small variations between them, such as A, AA, AAA, AAAA, AAAB, AAAC, AABA, and so on. If another user-specific data is submitted at login or stored in user profiles (such as an email address)
  - [ ] Check for session cookies and cookie expiration date/time
  - [ ] Identify cookie domain scope
  - [ ] Check for HttpOnly flag in cookie
  - [ ] Check for Secure flag in cookie if the application is over SSL
  - [ ] Check for session fixation i.e. value of session cookie before and after authentication
  - [ ] Replay the session cookie from a different effective IP address or system to check whether the server maintains the state of the machine or not
  - [ ] Check for concurrent login through different machine/IP
  - [ ] Check if any user pertaining information is stored in cookie value or not If yes, tamper it with other user's data
  - [ ] Failure to Invalidate Session on (Email Change,2FA Activation)
- **Authentication Testing**
  - [ ] Username enumeration
  - [ ] Bypass authentication using various SQL Injections on username and password field
  - Lack of password confirmation on
    - [ ] Change email address
    - [ ] Change password
    - [ ] Manage 2FA
  - [ ] Is it possible to use resources without authentication? Access violation
  - [ ] Check if user credentials are transmitted over SSL or not
  - [ ] Weak login function HTTP and HTTPS both are available
  - Test user account lockout mechanism on brute force attack

    Variation : If server blocks instant user requests, then try with time throttle option from intruder and repeat the process again.
    - [ ] Bypass rate limiting by tampering user agent to Mobile User agent
    - [ ] Bypass rate limiting by tampering user agent to Anonymous user agent
    - [ ] Bypass rate liniting by using null byte
  - [ ] Create a password wordlist using cewl command
  - Test Oauth login functionality
    - OAuth Roles
      - [ ] Resource Owner → User
      - [ ] Resource Server → Twitter

- [ ] Client Application → Twitterdeck.com
- [ ] Authorization Server → Twitter
- [ ] client_id → Twitterdeck ID (This is a public, non-secret unique identifier_
- [ ] client_secret → Secret Token known to the Twitter and Twitterdeck to generate access_tokens
- [ ] response_type → Defines the token type e.g (code, token, etc.)
- [ ] scope → The requested level of access Twitterdeck wants
- [ ] redirect_uri → The URL user is redirected to after the authorization is complete
- [ ] state → Main CSRF protection in OAuth can persist data between the user being directed to the authorization server and back again
- [ ] grant_type → Defines the grant_type and the returned token type
- [ ] code → The authorization code twitter generated, will be like ?code= , the code is used with client_id and client_secret to fetch an access_token
- [ ] access_token → The token twitterdeck uses to make API requests on behalf of the user
- [ ] refresh_token → Allows an application to obtain a new access_token without prompting the user

▼ Code Flaws

- [ ] Re-Using the code
- [ ] Code Predict/Bruteforce and Rate-limit
- [ ] Is the code for application X valid for application Y?

▼ Redirect_uri Flaws

- [ ] URL isn't validated at all: ?redirect_uri=https://attacker.com
- [ ] Subdomains allowed (Subdomain Takeover or Open redirect on those subdomains): ?redirect_uri=https://sub.twitterdeck.com
- [ ] Host is validated, path isn't (Chain open redirect): ?redirect_uri=https://twitterdeck.com/callback?redirectUrl=https://evil.com
- [ ] Host is validated, path isn't (Referer leakages): Include external content on HTML page and leak code via Referer
- [ ] Weak Regexes
- [ ] Bruteforcing the URL encoded chars after host: redirect_uri=https://twitterdeck.com§FUZZ§
- [ ] Bruteforcing the keywords whitelist after host (or on any whitelist open redirect filter): ?redirect_uri=https://§FUZZ§.com
- [ ] URI validation in place: use typical open redirect payloads

▼ State Flaws

- [ ] Missing State parameter? (CSRF)
- [ ] Predictable State parameter?
- [ ] Is State parameter being verified?

▼ Misc

- [ ] Is client_secret validated?
- [ ] Pre ATO using facebook phone-number signup
- [ ] No email validation Pre ATO

▼ Test 2FA Misconfiguration

- [ ] Response Manipulation
- [ ] Status Code
- [ ] Manipulation

- [ ] 2FA Code Leakage in Response
- [ ] 2FA Code Reusability
- [ ] Lack of Brute-Force Protection
- [ ] Missing 2FA Code Integrity Validation
- [ ] With null or 000000

▼ My Account (Post Login) Testing

- [ ] Find parameter which uses active account user id. Try to tamper it in order to change the details of the other accounts
- [ ] Create a list of features that are pertaining to a user account only. Change Email Change Password -Change account details (Name, Number, Address, etc.) Try CSRF
- [ ] Post login change email id and update with any existing email id. Check if its getting validated on server side or not. Does the application send any new email confirmation link to a new user or not? What if a user does not confirm the link in some time frame?
- [ ] Open profile picture in a new tab and check the URL. Find email id/user id info. EXIF Geolocation Data Not Stripped From Uploaded Images.
- [ ] Check account deletion option if application provides it and confirm that via forgot password feature
- [ ] Change email id, account id, user id parameter and try to brute force other user's password
- [ ] Check whether application re authenticates for performing sensitive operation for post authentication features

▼ Forgot Password Testing

- [ ] Failure to invalidate session on Logout and Password reset
- [ ] Check if forget password reset link/code uniqueness
- [ ] Check if reset link does get expire or not if its not used by the user for certain amount of time
- [ ] Find user account identification parameter and tamper Id or parameter value to change other user's password
- [ ] Check for weak password policy
- [ ] Weak password reset implementation Token is not invalidated after use
- [ ] If reset link has another param such as date and time, then. Change date and time value in order to make active & valid reset link
- [ ] Check if security questions are asked? How many guesses allowed? → Lockout policy maintained or not?
- [ ] Add only spaces in new password and confirmed password. Then Hit enter and see the result
- [ ] Does it display old password on the same page after completion of forget password formality?
- [ ] Ask for two password reset link and use the older one from user's email
- [ ] Check if active session gets destroyed upon changing the password or not?
- [ ] Weak password reset implementation Password reset token sent over HTTP
- [ ] Send continuous forget password requests so that it may send sequential tokens

▼ Contact Us Form Testing

- [ ] Is CAPTCHA implemented on contact us form in order to restrict email flooding attacks?
- [ ] Does it allow to upload file on the server?
- [ ] Blind XSS

▼ Product Purchase Testing

▼ Buy Now

- [ ] Tamper product ID to purchase other high valued product with low prize
- [ ] Tamper product data in order to increase the number of product with the same prize

▼ Gift/Voucher

- [ ] Tamper gift/voucher count in the request (if any) to increase/decrease the number of vouchers/gifts to be used
- [ ] Tamper gift/voucher value to increase/decrease the value of the voucher in terms of money. (e.g. $100 is given as a voucher, tamper value to increase, decrease money)
- [ ] Reuse gift/voucher by using old gift values in parameter tampering
- [ ] Check the uniqueness of gift/voucher parameter and try guessing other gift/voucher code
- [ ] Use parameter pollution technique to add the same voucher twice by adding same parameter name and value again with & in the BurpSuite request

▼ Add/Delete Product from Cart

- [ ] Tamper user id to delete products from other user's cart
- [ ] Tamper cart id to add/delete products from other user's cart
- [ ] Identify cart id/user id for cart feature to view the added items from other user's account

▼ Address

- [ ] Tamper BurpSuite request to change other user's shipping address to yours
- [ ] Try stored XSS by adding XSS vector on shipping address
- [ ] Use parameter pollution technique to add two shipping address instead of one trying to manipulate application to send same item on two shipping address

▼ Place Order

- [ ] Tamper payment options parameter to change the payment method. E.g. Consider some items cannot be ordered for cash on delivery but tampering request parameters from debit/credit/PayPal/net banking option to cash on delivery may allow you to
  place order for that particular item
- [ ] Tamper the amount value for payment manipulation in each main and sub requests and responses
- [ ] Check if CVV is going in cleartext or not
- [ ] Check if the application itself processes your card details and then performs a transaction or it calls any third-party payment processing company to perform a transaction

▼ Track Order

- [ ] Track other user's order by guessing order tracking number
- [ ] Brute force tracking number prefix or suffix to track mass orders for other users

▼ Wish list page testing

- [ ] Check if a user A can add/remote products in Wishlist of other user B's account
- [ ] Check if a user A can add products into user B's cart from his/her (user A's) Wishlist section.

▼ Post product purchase testing

- [ ] Check if user A can cancel orders for user B's purchase
- [ ] Check if user A can view/check orders already placed by user B
- [ ] Check if user A can modify the shipping address of placed order by user B

▼ Out of band testing

- [ ] Can user order product which is out of stock?

▼ **Banking Application Testing**

▼ Billing Activity

- [ ] Check if user 'A' can view the account statement for user 'B'
- [ ] Check if user 'A' can view the transaction report for user 'B'
- [ ] Check if user 'A' can view the summary report for user 'B'
- [ ] Check if user 'A' can register for monthly/weekly account statement via email behalf of user 'B'

- [ ] Check if user 'A' can update the existing email id of user 'B' in order to retrieve monthly/weekly account summary

- ▼ Deposit/Loan/Linked/External Account Checking
  - [ ] Check if user 'A' can view the deposit account summary of user 'B'
  - [ ] Check for account balance tampering for Deposit accounts
- ▼ Tax Deduction Inquiry Testing
  - [ ] Check if user 'A' with it's customer id 'a' can see the tax deduction details of user 'B' by tampering his/her customer id 'b'
  - [ ] Check parameter tampering for increasing and decreasing interest rate, interest amount, and tax refund
  - [ ] Check if user 'A' can download the TDS details of user 'B'
- [ ] Check if user 'A' can request for the cheque book behalf of user 'B'.
- ▼ Fixed Deposit Account Testing
  - [ ] Check if is it possible for user 'A' to open FD account behalf of user 'B'
  - [ ] Check if Can user open FD account with the more amount than the current account balance
- ▼ Stopping Payment on basis of cheque/date range
  - [ ] Can user 'A' stop the payment of user 'B' via cheque number
  - [ ] Can user 'A' stop the payment on basis of date range for user 'B'
- ▼ Status Enquiry Testing
  - [ ] Can user 'A' view the status enquiry of user 'B'
  - [ ] Can user 'A' modify the status enquiry of user 'B'
  - [ ] Can user 'A' post and enquiry behalf of user 'B' from his own account
- ▼ Fund transfer testing
  - [ ] Is it possible to transfer funds to user 'C' instead of user 'B' from the user 'A' which was intended to transfer from user 'A' to user 'B'
  - [ ] Can fund transfer amount be manipulated?
  - [ ] Can user 'A' modify the payee list of user 'B' by parameter manipulation using his/her own account
  - [ ] Is it possible to add payee without any proper validation in user 'A' 's own account or to user 'B' 's account
- ▼ Schedule transfer testing
  - [ ] Can user 'A' view the schedule transfer of user 'B'
  - [ ] Can user 'A' change the details of schedule transfer for user 'B'
- ▼ Testing of fund transfer via NEFT
  - [ ] Amount manipulation via NEFT transfer
  - [ ] Check if user 'A' can view the NEFT transfer details of user 'B'
- ▼ Testing for Bill Payment
  - [ ] Check if user can register payee without any checker approval
  - [ ] Check if user 'A' can view the pending payments of user 'B'
  - [ ] Check if user 'A' can view the payment made details of user 'B'

- ▼ **Open Redirection Testing**
  - ▼ Common injection parameters

```
/{payload}
?next={payload}
?url={payload}
?target={payload}
?rurl={payload}
```

```
?dest={payload}
?destination={payload}
?redir={payload}
?redirect_uri={payload}
?redirect_url={payload}
?redirect={payload}
/redirect/{payload}
/cgi-bin/redirect.cgi?{payload}
/out/{payload}
/out?{payload}
?view={payload}
/login?to={payload}
?image_url={payload}
?go={payload}
?return={payload}
?returnTo={payload}
?return_to={payload}
?checkout_url={payload}
?continue={payload}
?return_path={payload}
```

- [ ] Use burp 'find' option in order to find parameters such as URL, red, redirect, redir, origin, redirect_uri, target etc
- [ ] Check the value of these parameter which may contain a URL
- [ ] Change the URL value to www.tushar.com and check if gets redirected or not
- [ ] Try Single Slash and url encoding
- [ ] Using a whitelisted domain or keyword
- [ ] Using // to bypass http blacklisted keyword
- [ ] Using https: to bypass // blacklisted keyword
- [ ] Using \\ to bypass // blacklisted keyword
- [ ] Using \/\/ to bypass // blacklisted keyword
- [ ] Using null byte %00 to bypass blacklist filter
- [ ] Using ° symbol to bypass

▼ **Host Header Injection**

- [ ] Supply an arbitrary Host header
- [ ] Check for flawed validation
  - ▼ Send ambiguous requests
    - [ ] Inject duplicate Host headers
    - [ ] Supply an absolute URL
    - [ ] Add line wrapping
- [ ] Inject host override headers

▼ **SQL Injection Testin**

- ▼ Entry point detection
  - [ ] Simple characters
  - [ ] Multiple encoding
  - [ ] Merging characters
  - [ ] Logic Testing
  - [ ] Weird characters
- ▼ Use SQLmap to identify vulnerabile parameters
  - [ ] Fill form in browser GUI submit it normally
  - [ ] Go to history tab in burpsuite and find the relevent request
  - [ ] Right click and select the option "copy to file"
  - [ ] Save file as anyname.txt

- [ ] SQLmap command to run
- [ ] python sqlmap.py r ~/Desktop/textsqli.txt proxy= http://127.0.0.1:8080

- [ ] Run SQL injection scanner on all requests

▼ Bypassing WAF

- [ ] Using Null byte before SQL query
- [ ] Using SQL inline comment sequence
- [ ] URL encoding
- [ ] Changing Cases (uppercase/lowercase)
- [ ] Use SQLMAP tamper scripts

▼ Time Delays

```
Oracle        dbms_pipe.receive_message(('a'),10)

Microsoft     WAITFOR DELAY '0:0:10'

PostgreSQL    SELECT pg_sleep(10)

MySQL         SELECT sleep(10)
```

▼ Conditional Delays

```
Oracle        SELECT CASE WHEN (YOUR-CONDITION-HERE) THEN 'a'||dbms_pipe.receive_message(('a'),10) ELSE NULL END FROM du

Microsoft     IF (YOUR-CONDITION-HERE) WAITFOR DELAY '0:0:10'

PostgreSQL    SELECT CASE WHEN (YOUR-CONDITION-HERE) THEN pg_sleep(10) ELSE pg_sleep(0) END

MySQL         SELECT IF(YOUR-CONDITION-HERE,sleep(10),'a')
```

▼ **Cross-Site Scripting Testing**

- [ ] Try XSS using QuickXSS tool by theinfosecguy
- [ ] Upload file using '"><img src=x onerror=alert(document.domain)>.txt
- [ ] If script tags are banned, use <h1> and other HTML tags
- [ ] If output is reflected back inside the JavaScript as a value of any variable just use alert(1)
- [ ] if " are filtered then use this payload /><img src=d onerror=confirm(/tushar/);>
- [ ] Upload a JavaScript using Image file
- [ ] Unusual way to execute your JS payload is to change method from POST to GET. It bypasses filters sometimes

▼ Tag attribute value

- [ ] Input landed -<input type=”text” name=”state” value=”INPUT_FROM_ USER”>
- [ ] Payload to be inserted -“ onfocus=”alert(document.cookie)"

- [ ] Syntax Encoding payload “%3cscript%3ealert(document.cookie)%3c/script%3e"

▼ XSS filter evasion

- [ ] < and > can be replace with html entities < and >
- [ ] You can try an XSS polyglot.Eg:-javascript:/→*</title></style></textarea></script></xmp>* *<svg/onload='+/"/+/onmouseover=1/+/[/[]/+alert(1)//'>*

▼ XSS Firewall Bypass

- [ ] Check if the firewall is blocking only lowercase
- [ ] Try to break firewall regex with the new line(\r\n)
- [ ] Try Double Encoding

- [ ] Testing for recursive filters
- [ ] Injecting anchor tag without whitespaces
- [ ] Try to bypass whitespaces using Bullet
- [ ] Try to change request method

▼ **CSRF Testing**

- [ ] Validation of CSRF token depends on request method
- [ ] Validation of CSRF token depends on token being present
- [ ] CSRF token is not tied to the user session
- [ ] CSRF token is tied to a non-session cookie
- [ ] Validation of Referer depends on header being present

▼ **SAML Vulnerabilities**

- [ ] Signature Wrapping (XSW) Attacks
- [ ] SAML Message Integrity Abuse
- [ ] Missing / Invalid Signature
- [ ] SAML Message Replay
- [ ] Token Recipient Confusion

▼ **XML Injection Testing**

- [ ] Change the content type to text/xml then insert below code. Check via repeater

```
<?xml version="1.0" encoding="ISO 8859 1"?>
<!DOCTYPE tushar [
<!ELEMENT tushar ANY
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]><tushar>&xxe;</
<!ENTITY xxe SYSTEM "file:///etc/hosts" >]><tushar>&xxe;</
<!ENTITY xxe SYSTEM "file:///proc/self/cmdline" >]><tushar>&xxe;</
<!ENTITY xxe SYSTEM "file:///proc/version" >]><tushar>&xxe;</
```

- [ ] Blind XXE with out-of-band interaction

▼ **Cross-origin resource sharing (CORS)**

- [ ] Errors parsing Origin headers
- [ ] Whitelisted null origin value

▼ **Server-side request forgery (SSRF)**

▼ Common injection parameters

```
"access=",
"admin=",
"dbg=",
"debug=",
"edit=",
"grant=",
"test=",
"alter=",
"clone=",
"create=",
"delete=",
"disable=",
"enable=",
"exec=",
"execute=",
"load=",
"make=",
"modify=",
"rename=",
"reset=",
"shell=",
"toggle=",
"adm=",
"root=",
```

```
"cfg=",
"dest=",
"redirect=",
"uri=",
"path=",
"continue=",
"url=",
"window=",
"next=",
"data=",
"reference=",
"site=",
"html=",
"val=",
"validate=",
"domain=",
"callback=",
"return=",
"page=",
"feed=",
"host=",
"port=",
"to=",
"out=",
"view=",
"dir=",
"show=",
"navigation=",
"open=",
"file=",
"document=",
"folder=",
"pg=",
"php_path=",
"style=",
"doc=",
"img=",
"filename="
```

- [ ] Try basic localhost payloads

▼ Bypassing filters

- [ ] Bypass using HTTPS
- [ ] Bypass with [::]
- [ ] Bypass with a domain redirection
- [ ] Bypass using a decimal IP location
- [ ] Bypass using IPv6/IPv4 Address Embedding
- [ ] Bypass using malformed urls
- [ ] Bypass using rare address(short-hand IP addresses by dropping the zeros)
- [ ] Bypass using enclosed alphanumerics

▼ Cloud Instances

▼ AWS

```
http://instance-data
http://169.254.169.254
http://169.254.169.254/latest/user-data
http://169.254.169.254/latest/user-data/iam/security-credentials/[ROLE NAME]
http://169.254.169.254/latest/meta-data/
http://169.254.169.254/latest/meta-data/iam/security-credentials/[ROLE NAME]
http://169.254.169.254/latest/meta-data/iam/security-credentials/PhotonInstance
http://169.254.169.254/latest/meta-data/ami-id
http://169.254.169.254/latest/meta-data/reservation-id
http://169.254.169.254/latest/meta-data/hostname
http://169.254.169.254/latest/meta-data/public-keys/
http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
http://169.254.169.254/latest/meta-data/public-keys/[ID]/openssh-key
http://169.254.169.254/latest/meta-data/iam/security-credentials/dummy
http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
http://169.254.169.254/latest/dynamic/instance-identity/document
```

▼ Google Cloud

```
http://169.254.169.254/computeMetadata/v1/
http://metadata.google.internal/computeMetadata/v1/
http://metadata/computeMetadata/v1/
http://metadata.google.internal/computeMetadata/v1/instance/hostname
http://metadata.google.internal/computeMetadata/v1/instance/id
http://metadata.google.internal/computeMetadata/v1/project/project-id
```

▼ Digital Ocean

```
curl http://169.254.169.254/metadata/v1/id
http://169.254.169.254/metadata/v1.json
http://169.254.169.254/metadata/v1/
http://169.254.169.254/metadata/v1/id
http://169.254.169.254/metadata/v1/user-data
http://169.254.169.254/metadata/v1/hostname
http://169.254.169.254/metadata/v1/region
http://169.254.169.254/metadata/v1/interfaces/public/0/ipv6/address
```

▼ Azure

```
http://169.254.169.254/metadata/v1/maintenance
http://169.254.169.254/metadata/instance?api-version=2017-04-02
http://169.254.169.254/metadata/instance/network/interface/0/ipv4/ipAddress/0/publicIpAddress?api-version=2017-04-02&f
ormat=text
```

- [ ] Bypassing via open redirection

▼ **File Upload Testing**

- [ ] upload the malicious file to the archive upload functionality and observe how the application responds
- [ ] upload a file and change its path to overwrite an existing system file
- [ ] Large File Denial of Service
- [ ] Metadata Leakage
- [ ] ImageMagick Library Attacks
- [ ] Pixel Flood Attack

▼ Bypasses

- [ ] Null Byte (%00) Bypass
- [ ] Content-Type Bypass
- [ ] Magic Byte Bypass
- [ ] Client-Side Validation Bypass
- [ ] Blacklisted Extension Bypass
- [ ] Homographic Character Bypass

▼ **CAPTCHA Testing**

- [ ] Missing Captcha Field Integrity Checks
- [ ] HTTP Verb Manipulation
- [ ] Content Type Conversion
- [ ] Reusuable Captcha
- [ ] Check if captcha is retrievable with the absolute path such as www.tushar.com/internal/captcha/images/24.png
- [ ] Check for the server side validation for CAPTCHA.Remove captcha block from GUI using firebug addon and submit request to the server
- [ ] Check if image recognition can be done with OCR tool?

▼ **JWT Token Testing**

- [ ] Brute-forcing secret keys
- [ ] Signing a new token with the “none” algorithm
- [ ] Changing the signing algorithm of the token (for fuzzing purposes)
- [ ] Signing the asymmetrically-signed token to its symmetric algorithm match (when you have the original public key)

▼ **Websockets Testing**

- [ ] Intercepting and modifying WebSocket messages
- [ ] Websockets MITM attempts
- [ ] Testing secret header websocket
- [ ] Content stealing in websockets
- [ ] Token authentication testing in websockets

▼ **GraphQL Vulnerabilities Testing**

- [ ] Inconsistent Authorization Checks
- [ ] Missing Validation of Custom Scalars
- [ ] Failure to Appropriately Rate-limit
- [ ] Introspection Query Enabled/Disabled

▼ **WordPress Common Vulnerabilities**

- [ ] XSPA in wordpress
- [ ] Bruteforce in wp-login.php
- [ ] Information disclosure wordpress username
- [ ] Backup file wp-config exposed
- [ ] Log files exposed
- [ ] Denial of Service via load-styles.php
- [ ] Denial of Service via load-scripts.php
- [ ] DDOS using xmlrpc.php

▼ **Denial of Service**

- [ ] Cookie bomb
- [ ] Pixel flood, using image with a huge pixels
- [ ] Frame flood, using GIF with a huge frame
- [ ] ReDoS (Regex DoS)
- [ ] CPDoS (Cache Poisoned Denial of Service)

▼ **Other Test Cases (All Categories)**

▼ Check for security headers and at least

- [ ] X Frame Options
- [ ] X-XSS header
- [ ] HSTS header
- [ ] CSP header
- [ ] Referrer Policy
- [ ] Cache Control
- [ ] Public key pins

▼ Testing for Role authorization

- [ ] Check if normal user can access the resources of high privileged users?

- [ ] Forced browsing
- [ ] Insecure direct object reference
- [ ] Parameter tampering to switch user account to high privileged user

▼ Blind OS command injection

- [ ] using time delays
- [ ] by redirecting output
- [ ] with out-of-band interaction
- [ ] with out-of-band data exfiltration

- [ ] Command injection on CSV export (Upload/Download)
- [ ] CSV Excel Macro Injection
- [ ] If you find phpinfo.php file, check for the configuration leakage and try to exploit any network vulnerability.
- [ ] Parameter Pollution Social Media Sharing Buttons

▼ Broken Cryptography

- [ ] Cryptography Implementation Flaw
- [ ] Encrypted Information Compromised
- [ ] Weak Ciphers Used for Encryption

▼ Web Services Testing

- [ ] Test for directory traversal
- [ ] Web services documentation disclosure Enumeration of services, data types, input types boundaries and limits

Created by: Tushar Verma(e11i0t_4lders0n)

Contact Me: LinkedIn ,Twitter

Most Comprehensive Web Application Penetration Testing Checklist

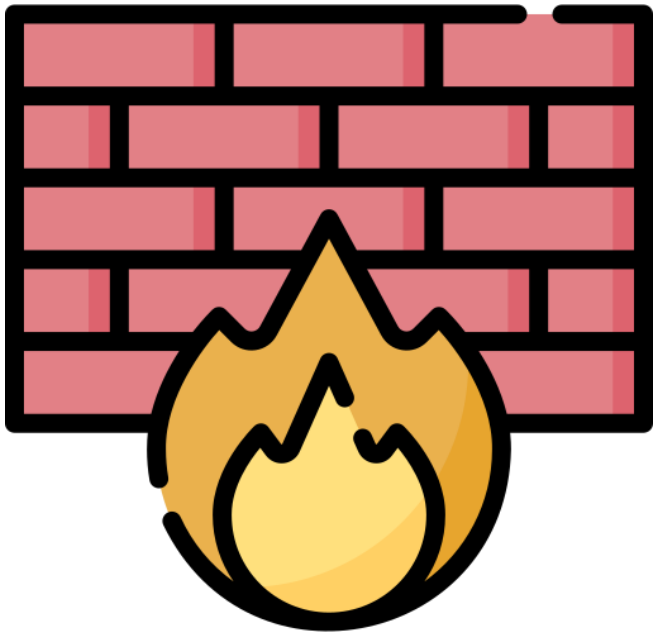
More than 170 custom testcases

Prepared by: Chintan Gurjar

1. Fingerprinting Application

- Bruteforce subdomains
- Directory enumeration via Dirb, Dirbuster, BurpSuite Intruder, etc.
- Identidy underlying web client and server technology
- Uncover HTTP/HTTPs services running on ports other than the 80 and 443
- Find leaked email id, passwords using ‘We leak Info’ and ‘Hunter.io’
- Identidy firewall
- Find sensitive information through keywords after crawling entire site. Keywords such as admin, password, todo, http

2. Network Testing



- Test for ping (ICMP packets are allowed or filtered)
- DNS testing for zone transfer, missing DNSSEC policies
- Missing DMARC policies
- Perform Nessus scan
- Banner disclosure for open ports and network services
- Find all web and network services other than port 80 and 443
- Perform UDP scan using UDP proto scanner

3. Application Features Mapping

- Generate site structure in any mindmap tool
- List all dynamic features
- Add all possible theoritical test cases within your mind map for testing security of those features

4. Application Component Audit

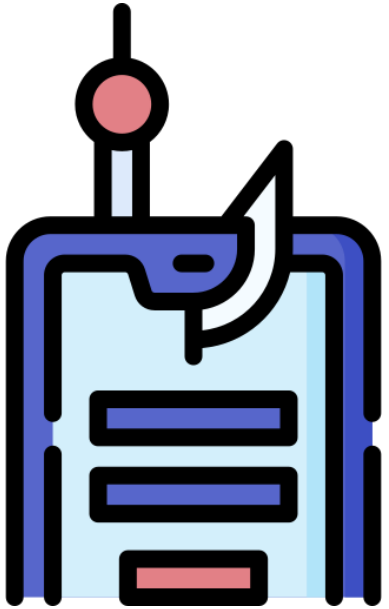
- Test SSL/TLS weaknesses using Qualys SSL scanner
- Identify known vulnerabilities in running web and network components using known CVE, searchsploits, Metasploit auxiliaries and exploits

Prepared by: Chintan Gurjar

Chintangurjar@outlook.com
@iamthefrogy
Linkedin – Chintan Gurjar

5. Session Management Testing

- Identify actual session cookie out of bulk cookies in the application.
- Decode cookies using some standard decoding algorithms such as Base64, hex, URL etc.
- Modify cookie.session token value by 1 bit/byte. Then resubmit and do the same for all token. Reduce the amount of work you need to perform in order to identify which part of token is actually being used and which is not.
- If self-registration is available and you can choose your username, log in with a series of similar usernames containing small variations between them, such as A, AA, AAA, AAAA, AAAB, AAAC, AABA, and so on. If other user-specific data is submitted at login or stored in user profiles (such as an e-mail address)
- Token leakage via Referer header - Untrusted 3rd Party
- Check for session cookies and cookie expiration date/time
- Identify cookie domain scope
- Check for HttpOnly flag in cookie
- Check for Secure flag in cookie if the application is over SSL
- Check for session fixation i.e. value of session cookie before and after authentication
- Replay the session cookie from a different effective IP address or system to check whether server maintains the state of the machine or not.
- Check for concurrent login through different machine/IP
- Check if any user pertaining information is stored in cookie value or not If yes, tamper it with other user's data.

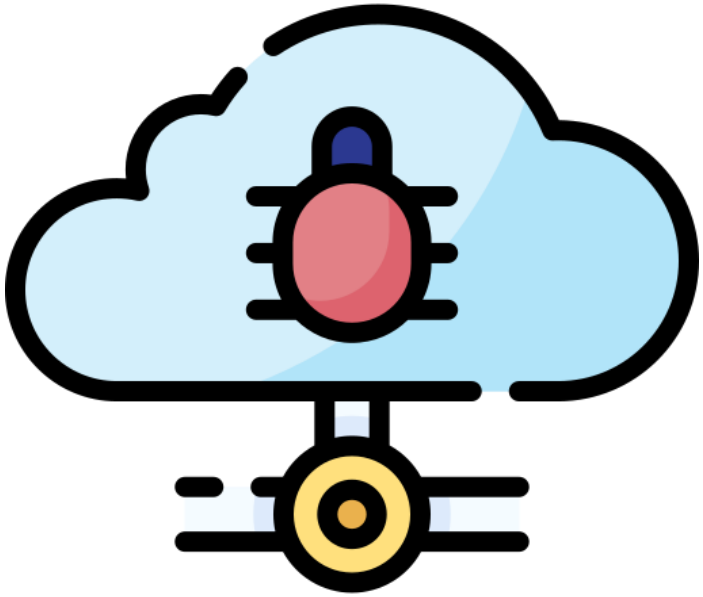


Prepared by: Chintan Gurjar

Chintangurjar@outlook.com
@iamthefrogy
Linkedin – Chintan Gurjar

6. Registration Feature Testing

- Check for duplicate registration / Overwrite existing user
- Check for weak password policy
- Check for the stored chintan in username, account name for registration.
- Check for insufficient email verification process
- Weak registration implementation - Allows disposable email addresses
- Overwrite default web application pages by specially crafted username registrations. => After registration, does your profile link appears something as www.chintan.com/chintan ? a. If so, enumerate default folders of web application such as /images, /contact, /portfolio b. Do a registration using the username such as images, contact, portfolio c. Check if those default folders have been overwritten by your profile link or not."



Prepared by: Chintan Gurjar

Chintangurjar@outlook.com
@iamthefrogy
Linkedin – Chintan Gurjar

7. Authentication Testing

- Username enumeration
- Bypass authentication using various SQL Injections on username and password field. Use combinations of below injections chintan' -- chintan' # chintan'/* ' or 1=1 -- ' or 1=1 # ' or 1=1/* ') or '1'='1 -- ') or ('1'='1 --"
- Auto-complete testing
- Lack of password confirmation on
    - Change email address
    - Change password
    - Manage 2FA
- Is it possible to use resources without authentication? Access violation
- Check if user credentials are transmitted over SSL or not.
- Weak login function - HTTP and HTTPS both are available.
- Test user account lockout mechanism on brute force attack
    - Variation : If server blocks instant user requests, then try with time throttle option from intruder and repeat the process again.
        - Bypass rate limiting by tampering user agent to Mobile User agent.
        - Bypass rate limiting by tampering user agent to Anonymous user agent.
- Create a password wordlist using cewl command
- Test 0auth login functionality for Open Redirection
    - Use burp 'find' option in order to find parameters such as URL, red, redirect, redir, origin,dest, targetURL, checkout_URL etc.
    - Check the value of these parameter which may contain a URL.
    - Check open redirection for 0auth functionality.
    - Change the URL value to www.chintan.com and check if gets redirected or not. 5) Check if same secret code request can be used multiple times."

Prepared by: Chintan Gurjar

Chintangurjar@outlook.com
@iamthefrogy
Linkedin – Chintan Gurjar

8. Error Codes Testing

- Generate custom pages such as /chintan.php, chintan.aspx and identify error page
- Add multiple parameters in same post get request using different value and generate error
- Add [],]], and [[in cookie values and parameter values to create errors
- Try to generate unusual error code by giving input as /~chintan/%s at the end of website URL
- Fuzz using the Burp Intruder with malicious input and try to generate error codes

9. My Account (Post Login) Testing

- Find parameter which uses active account user id. Try to tamper it in order to change the details of other account.
- Create a list of features that are pertaining to a user account only.- Change Email- Change Password- Change account details (Name, Number, Address, etc.) Try CSRF
- Post login change email id and update with any existing email id. Check if its getting validated on server side or not. Does the application send any new email confirmation link to a new user or not? What if a user does not confirm the link in some time frame?
- Perform all file upload test using extension tampering and file content modifying. Unsafe File upload - - No Antivirus - No Size Limit - File extension Filter Bypass
- Open profile picture in new tab and check the URL. Find email id/user id info. EXIF Geolocation Data Not Stripped From Uploaded Images.
- Check account deletion option if application provides it and confirm that via forgot password feature
- Change email id, account id, user id parameter and try to brute force other user's password
- Check whether application re-authenticates for performing sensitive operation for post authentication features

Prepared by: Chintan Gurjar

Chintangurjar@outlook.com
@iamthefrogy
Linkedin – Chintan Gurjar

10. Forgot Password Testing

- Failure to invalidate session on Logout and Password reset
- Check if forget password reset link/code uniqueness
- Check if reset link does get expire or not if its not used by the user for certain amount of time
- Find user account identification parameter and tamper Id or parameter value to change other user's password
- Check for weak password policy
- Weak password reset implementation - Token is not invalidated after use
- If reset link have another params such as date and time, then. Change date and time value in order to make active & valid reset link.
- Check if security questions are asked? How many guesses allowed? -> Lockout policy maintained or not?
- Add only spaces in new password and confirmed password. Then Hit enter and see the result.
- Does it display old password on the same page after completion of forget password formality?
- Ask for two password reset link and use the older one from user's email
- Check if active session gets destroyed upon changing the password or not?
- Weak password reset implementation - Password reset token sent over HTTP
- Send continuous forget password requests so that it may send sequential tokens

11. Contact Us Form Testing

- Is CAPTCHA implemented on contact us form in order to restrict email flooding attacks?
- Does it allow to upload file on the server?

Prepared by: Chintan Gurjar

Chintangurjar@outlook.com
@iamthefrogy
Linkedin – Chintan Gurjar

12. Product Purchase Testing

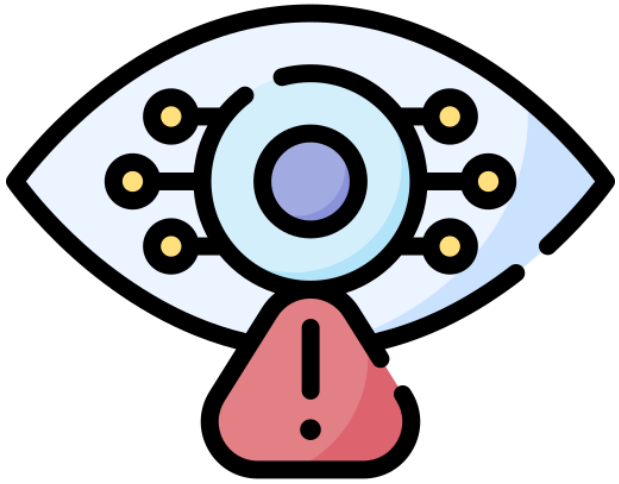
- **Buy Now**
  - Tamper product ID to purchase other high valued product with low prize
  - Tamper product data in order to increase the number of product with the same prize
- **Gift / Voucher**
  - Tamper gift/voucher count in the request (if any) to increase/decrease the number of vouchers/gifts to be used
  - Tamper gift/voucher value to increase/decrease the value of voucher in terms of money. (e.g. $100 is given as a voucher, tamper value to increase, decrease money)
  - Reuse gift/voucher by using old gift values in parameter tampering.
  - Check the uniqueness of gift/voucher parameter and try guessing other gift/voucher code.
  - Use parameter pollution technique to add same voucher twice by adding same parameter name and value again with & in the BurpSuite request.
- **Add/Delete Product from Cart**
  - Tamper user id to delete products from other user's cart.
  - Tamper cart id to add/delete products from other user's cart.
  - Identify cart id/user id for cart feature to view the added items from other user's account.
- **Address**
  - Tamper BurpSuite request to change other user's shipping address to yours.
  - Try stored-XSS by adding XSS vector on shipping address.
  - Use parameter pollution technique to add two shipping address instead of one trying to manipulate application to send same item on two shipping address.
- **Place Order**
  - Tamper payment options parameter to change the payment method. E.g. Consider some items cannot be ordered for cash on delivery but tampering request parameters from debit/credit/PayPal/net banking option to cash on delivery may allow you to place order for that particular item.
  - Tamper the amount value for payment manipulation in each main and sub requests and responses.
  - Check if CVV is going in cleartext or not.
  - Check if credit/debit card details are masked or not.
  - Check if application itself process your card details and then perform transaction or it calls any third party payment processing company to perform transaction.
- **Track Order**
  - Track other user's order by guessing order tracking number

Prepared by: Chintan Gurjar

Chintangurjar@outlook.com
@iamthefrogy
Linkedin – Chintan Gurjar

13. Flight/Railway/Hotel Booking Testing

- **Booking details**
  - View/Manage other user's booking details.
  - Check reservation status for other users/behalf of other users.
- **Ticket/Voucher**
  - View other users vouchers/e-tickets from PRINT option
  - Check if sensitive data is passed in GET request
  - If e-ticket/voucher is sent on email then check for the email flooding attack.
- **Refund**
  - View other user's refund status.
  - Refund more money than the intended one by parameter manipulation.
  - If refund tracking is allowed then gain other user's refund tracking status.
- **Cancellation**
  - Gain higher cancellation amount with parameter modifying for amount value.
- **Booking**
  - Do 1st person booking and add 3 other persons in same prize
  - Hotel - Book normal room - Select Deluxe room in the same prize



Prepared by: Chintan Gurjar

Chintangurjar@outlook.com
@iamthefrogy
Linkedin – Chintan Gurjar

14. Cross-Site Scripting Testing

- Locator: ';!--"<chintan>=&{()}
- Try XSS using XSSstrike tool by Somdev Sangwan
- Upload file using '"><img src=x onerror=alert(document.domain)>.txt
- Standard payload for URI and all inputs:
  - "><img src=x onerror=prompt(document.cookie);><!--
  - "><img src=x onerror=confirm(document.cookie);><!--
  - "><img src=x onerror=alert(document.cookie);><!--
- If script tags are banned, use <h1> and other HTML tags
- If output is reflected back inside the JavaScript as a value of any variable just use alert(1)
- if " are filtered then use this payload /><img src=d onerror=confirm(/chintan/);>
- Upload a JavaScript using Image file
- Unusual way to execute your JS payload is to change method from POST to GET. It bypasses filters sometimes.
- Tag attribute value
  - Input landed - <input type="text" name="state" value="INPUT_FROM_ USER">
  - Payload to be inserted - " onfocus="alert(document.cookie)"
- Syntax Encoding payload "%3cscript%3ealert(document.cookie)%3c/script%3e"
- ASP.NET IE9 chintan Filter evasion for htmlentities
  - <%tag style="chintan:expression(alert('chintan'))">
  - ‹%tag style="chintan:expression(alert(123))
  - ‹%tag style="chintan:expression(alert(123))"
- Try base64 payload
- If the logout button just performs the redirection then use old classic XSS payload
- Polyglot payload
- Use pure JS payload that worked for many popular websites if your input is reflected back in the JavaScript.

Prepared by: Chintan Gurjar

Chintangurjar@outlook.com
@iamthefrogy
Linkedin – Chintan Gurjar

15. SQL Injection Testing

- Locator (Error Based)
  - Test'"" 123' ""Þ}j%Ùÿ'"""""""""';' '""();=,%+-/**/ --«
- If parameter=static_integer_value then follow below method. If id=4, then try id=3+1 or id=6-2 (if page loads in same way, it is vulnerable)
- Use SQLmap to identify vulnerabile parameters
  - Fill form in browser GUI submit it normally.
  - Go to history tab in burpsuite and find the relevent request.
  - Right click and select the option "copy to file".
  - Save file as anyname.txt
  - SQLmap command to run
  - python sqlmap.py -r ~/Desktop/textsqli.txt --proxy=http://127.0.0.1:8080
- Run SQL injection scanner on all requests

16. Open Redirection Testing

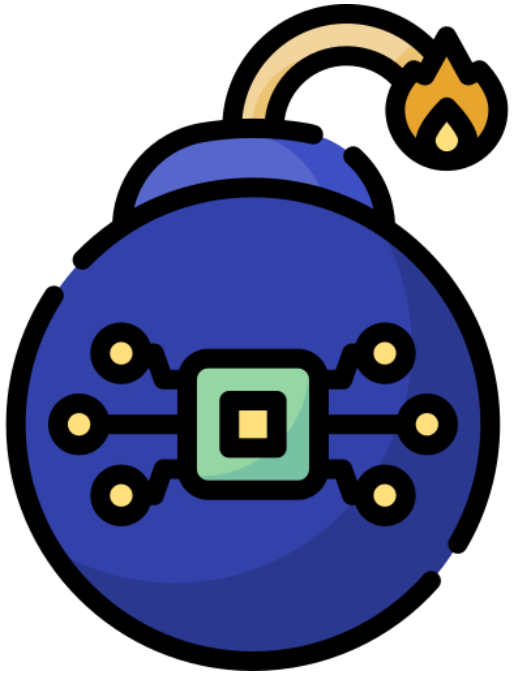
- Use burp 'find' option in order to find parameters such as URL, red, redirect, redir, origin, redirect_uri, target etc.
- Check the value of these parameter which may contain a URL.
- Change the URL value to www.chintan.com and check if gets redirected or not.
- Give below URL in web browser and check if application redirects to the www.chintan.com website or not.
  - https://www.target.com/ÿ/www.twitter.com/
  - https://www.target.com//www.twitter.com/
  - https://www.target.com/Ã¿/www.twitter.com/
  - https://www.target.com//www.twitter.com/
- Bypass filter using returnTo=///chintan.com/
- Bypass filter using returnTo=http:///chintan.com/

Prepared by: Chintan Gurjar

Chintangurjar@outlook.com
@iamthefrogy
Linkedin – Chintan Gurjar

17. Host Header Injection

- Inset new header in the GET/POST request as follows:
  X-Forwarded-Host: www.chintan.com
  If it gets redirected from the target application then its vulnerable
  Capture any request,
  Change the host to google.com and see if its getting redirected or not



18. ASP.NET Application Testing

- Check if ASP.net viewstate parameter is encrypted or not
- Check if any ASP configuration is disclosed publicly or not
- Check if error codes reveal the version of ASP.NET used in the application

19. CSRF Testing

- Re-use Anti-CSRF token for CSRF attack
- Check if token is validated on server side or not
- Check if token validation for full length or partial length
- Create few dummy account and compare the CSRF token for all those accounts
- Bypass CSRF token using 2 input type fields in for updating user's information in the same HTML file
- Convert POST request to GET and remove _csrf (anti-csrf token) to bypass the CSRF protection.
- Check if the value you are trying to change is passed in multiple parameters such as cookie, http headers along with GET and POST request.

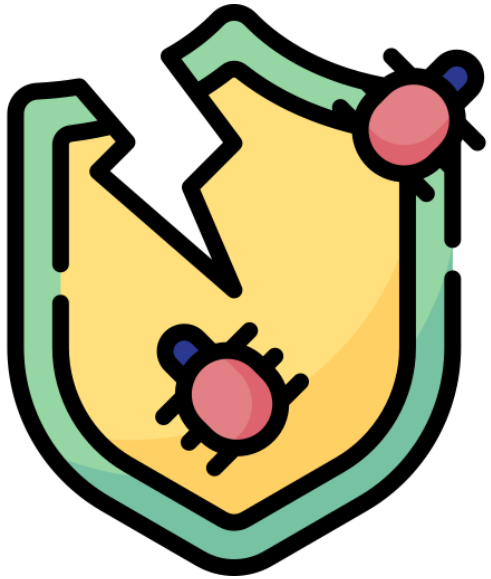
Prepared by: Chintan Gurjar

Chintangurjar@outlook.com
@iamthefrogy
Linkedin – Chintan Gurjar

20. XML Injection Testing

- Change the content type to text/xml then insert below code. Check via repeater

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE chintan [
<!ELEMENT chintan ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]><chintan>&xxe;</foo>
```



21. Web Services Testing

- SOAP Message Tampering
  - Brute forcing using *
  - Brute forcing using user credentials
  - Parameter guessing
- SQL injection using ' " - *)
- Test for directory traversal
- Test for XML poisoning
- Web services documentation disclosure – Enumeration of services, data types, input types boundaries and limits

22. Automated Scanner

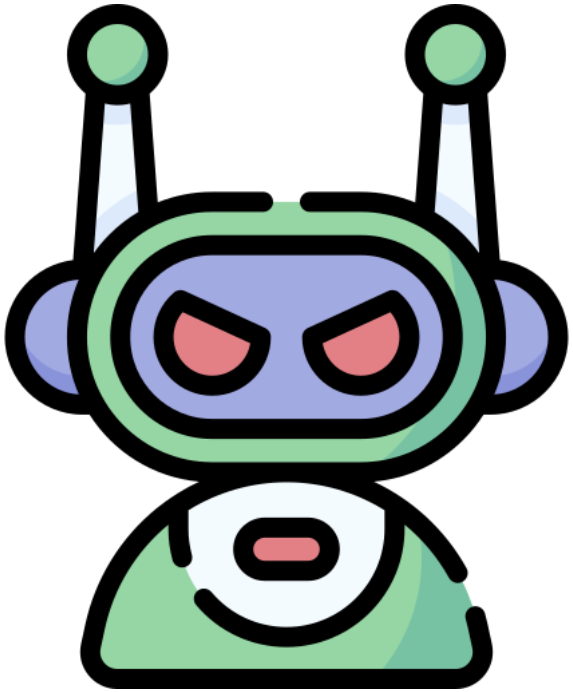
- Run automated scanner at least
  - Netsparker
  - BurpSuite Scanner
  - For WordPress – Pecan; For Joomla – Groomsman
  - Nessus for network services scan
  - Nexpose for network services scan

Prepared by: Chintan Gurjar

Chintangurjar@outlook.com
@iamthefrogy
Linkedin – Chintan Gurjar

22. CAPTCHA Testing

- Replay attack
  - Send old captcha value with if accepts then it is vulnerable.
  - Send old captcha value with old session ID, if its accepts then it is vulnerable.
- Check if captcha is retrievable with the absolute path such as www.chintan.com/internal/captcha/images/24.png
- Check for the server-side validation for CAPTCHA. Remove captcha block from GUI using firebug addon and submit request to the server.
- Check if image recognition can be done with OCR tool?
  - If OCR identifies then report as weak strength of captcha - OCR (Optical Character Recognition)



Prepared by: Chintan Gurjar

Chintangurjar@outlook.com
@iamthefrogy
Linkedin – Chintan Gurjar

23. Other Test Cases (All Categories)

- Check for SSRF Vulnerability by giving www.chintan.com:22 , www.chintan.com:23 etc. Check for the response page and determine if port 22 is opened in chintan website. If yes then target website is vulnerable to SSRF vulnerability.
- Check for security headers and at least:
  - X-Frame-Options
  - X-XSS header
  - HSTS header
  - CSP header
  - Referrer-Policy
  - Cache Control
  - Public key pins
- Command injection on CSV export (Upload/Download)
- DDOS using xmlrpc.php
- If website has a feature for importing contacts from .CSV files then
  - Add one contact in your CSV file with the name "><script>alert("chintan")</script>
  - Import contact to the website
  - Check if script getting executed or not.
- CSV Excel Macro Injection
- Find metadata for the downloadable objects
- Review Image files, PDF files and other object's metadata for information leakage
- Test Rich Internet Application RIA cross domain policy; Try to access crossdomain.xml; Try to access clientaccesspolicy.xml
- If you find phpinfo.php file, check for the configuration leakage and try to exploit any network vulnerability.
- Bypass SAML authentication by response tampering

Prepared by: Chintan Gurjar

Chintangurjar@outlook.com
@iamthefrogy
Linkedin – Chintan Gurjar

23. Other Test Cases (All Categories) Cont...

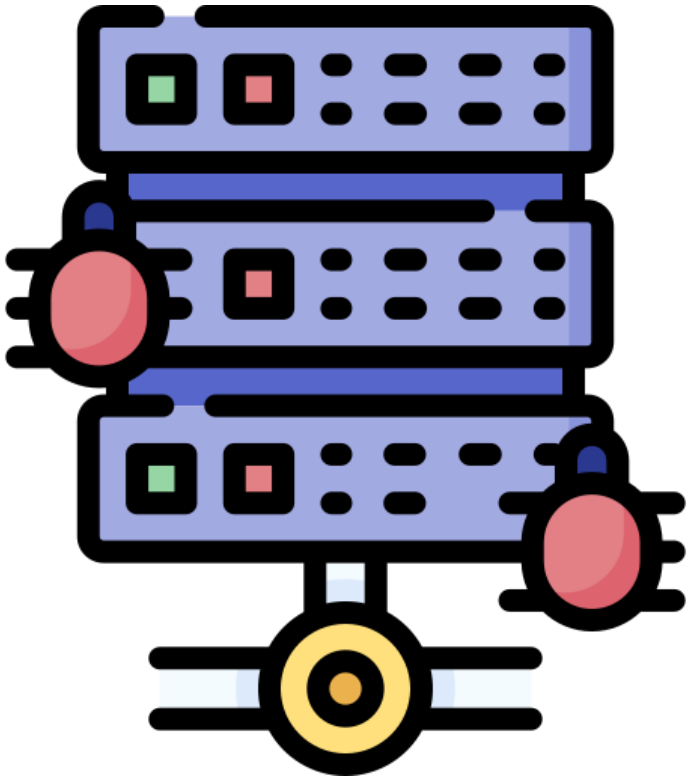
- Testing for Role authorization
  - Check if normal user can access the resources of high privileged users?
  - Forced browsing
  - Insecure direct object reference
  - Parameter tampering to switch user account to high privileged user.
- Test for OTP
  - Try injection to bypass OTP verification
  - Check for guessable OTP codes
  - Check for the response in order to bypass OTP.
  - Give ' in OTP and check if you can bypass it or not.
- If CSP header blocks the clickjacking attack and origin parameter is present in the original request then this scenario can be bypassed by adding Unicode characters in the value of origin header.
- Use PATCH HTTP header to find information disclosure
- Check whether the application uses any ip address parameter or not. If yes, then decimal IP address can be converted into real ip for information disclosure.
- Imagemagick GIF coder vulnerability leads to memory disclosure
- If the GIT repository file is found on the server, then try to download the entire source code of the website using git-dumper tool.
- Check for the Unsubscribe button
  - Subscribe to email id
  - Unsubscribe and check whether the website confirms first or sends any notification to a user or not.
  - if yes - Not vulnerable
  - if no - Vulnerable (affects availability)
  - If a website has username enumeration issue then it becomes High-Medium level issue.

Prepared by: Chintan Gurjar

Chintangurjar@outlook.com
@iamthefrogy
Linkedin – Chintan Gurjar

23. Other Test Cases (All Categories) Cont...

- Executable download - No secure integrity check
- Reflected file download
- Parameter Pollution - Social Media Sharing Buttons
- Full path disclosure
- Internal Ip disclosure
- Outdated software versions
- Sensitive application data stored unencrypted - Internal storage
- Unsafe Cross-Origin-Resource Sharing
- Directory listing - Non sensitive data exposure.
- Potentially unsafe HTTP method enabled
  - OPTIONS PUT DELETE
- If the server is IIS 7 then test for
  - IIS Short Name scanner
  - HTTP.sys DOS RCE
- WordPress testing
  - enumerate vulnerable plugins
  - enumerate vulnerable themes
  - enumerate email addresses and usernames
  - brute force using custom wordlist using WordPress
- Use Metasploit to find custom exploits
  - use Metasploit --check option to check whether target is exploitable or not
  - remember to give targetURI for the successful exploitation



Prepared by: Chintan Gurjar

Chintangurjar@outlook.com
@iamthefrogy
Linkedin – Chintan Gurjar

24. Websockets Testing

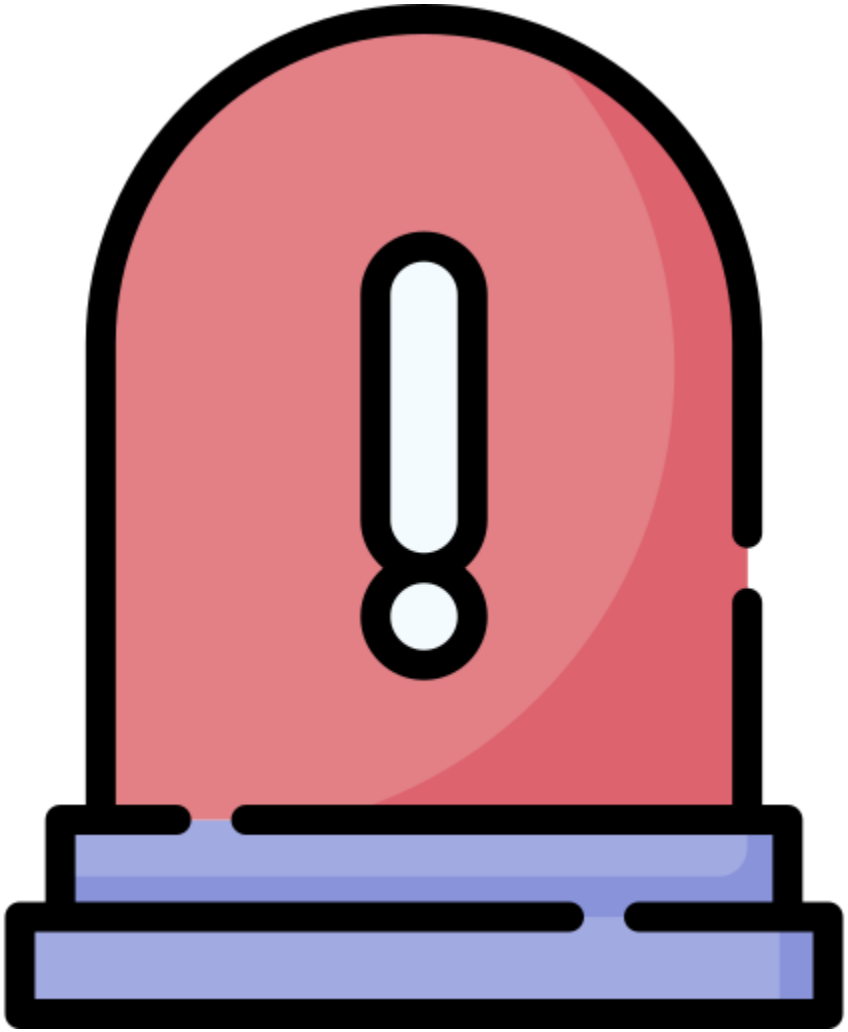
- Intercepting websockets messaging
- Websockets MITM attempts
- XSS on websockets
- Testing secret header websocket
- Content stealing in websockets
- Token authentication testing in websockets

25. JWT Token Testing

- Testing for any leaked secret
- Dictionary attack on token
- Exploiting the 'None' algorithm
- Abusing transaction replay
- Abusing key management
- Testing for debug mode
- Testing weak signing key

25. API Testing

- Abusing object level authentication
- Abusing weak password/dictionary brute forcing
- Testing for mass management
- Testing for excessive data exposure
- Testing for command injection
- Testing for misconfigured permissions
- Testing for SQL injection



Prepared by: Chintan Gurjar

Chintangurjar@outlook.com
@iamthefrogy
LinkedIn – Chintan Gurjar

26. Banking Application Testing

- Billing Activity
  - Check if user 'A' can view the account statement for user 'B'
  - Check if user 'A' can view the transaction report for user 'B'
  - Check if user 'A' can view the summary report for user 'B'
  - Check if user 'A' can register for monthly/weekly account statement via email behalf of user 'B'
  - Check if user 'A' can update the existing email id of user 'B' in order to retrieve monthly/weekly account summary
- Deposit/Loan/Linked/External Account Checking
  - Check if user 'A' can view the deposit account summary of user 'B'
  - Check for account balance tampering for Deposit accounts.
- Tax Deduction Inquiry Testing
  - Check if user 'A' with it's customer id 'a' can see the tax deduction details of user 'B' by tampering his/her customer id 'b'
  - Check parameter tampering for increasing and decreasing interest rate, interest amount, and tax refund.
  - Check if user 'A' can download the TDS details of user 'B'.
- Check if user 'A' can request for the cheque book behalf of user 'B'.
- Fixed Deposit Account Testing
  - Check if is it possible for user 'A' to open FD account behalf of user 'B'.
  - Check if Can user open FD account with the more amount than the current account balance.
- Stopping Payment on basis of cheque/date range
  - Can user 'A' stop the payment of user 'B' via cheque number.
  - Can user 'A' stop the payment on basis of date range for user 'B'

Prepared by: Chintan Gurjar

Chintangurjar@outlook.com
@iamthefrogy
LinkedIn – Chintan Gurjar

26. Banking Application Testing Cont...

- Status Enquiry Testing
  - Can user 'A' view the status enquiry of user 'B'
  - Can user 'A' modify the status enquiry of user 'B'
  - Can user 'A' post and enquiry behalf of user 'B' from his own account.
- Fund transfer testing
  - Is it possible to transfer funds to user 'C' instead of user 'B' from the user 'A' which was intended to transfer from user 'A' to user 'B'
  - Can fund transfer amount be manipulated?
  - Can user 'A' modify the payee list of user 'B' by parameter manipulation using his/her own account.
  - Is it possible to add payee without any proper validation in user 'A' 's own account or to user 'B' 's account.
- Schedule transfer testing
  - Can user 'A' view the schedule transfer of user 'B'
  - Can user 'A' change the details of schedule transfer for user 'B'
- Testing of fund transfer via NEFT
  - Amount manipulation via NEFT transfer.
  - Check if user 'A' can view the NEFT transfer details of user 'B'.
- Testing for Bill Payment
  - Check if user can register payee without any checker approval
  - Check if user 'A' can view the pending payments of user 'B'
  - Check if user 'A' can view the payment made details of user 'B'

Prepared by: Chintan Gurjar

Chintangurjar@outlook.com
@iamthefrogy
LinkedIn – Chintan Gurjar

Wildcard Domain Recon Checklist (Based on 0xpatrick Workflow)

Recon on Wildcard Domain

Subdomain Enumeration

- Run Amass
- Run Subfinder
- Run Rapid7 FDNS
- Use commonspeak2 list
- Run massdns
- Run altdns
- Run massdns

Single Domain Scanning

- Arachni Scan
- OWASP ZAP Scan
- Burp Spider
- Burp Scanning
- Wayback Machine
- Linkfinder
- URL with Android application

Manual Checking

- Shodan
- Censys
- Google dorks
- Pastebin

- Github

- OSINT

Information Gathering

- Manually explore the site

- Spider/crawl for hidden content

- Check robots.txt, sitemap.xml, .DS_Store

- Check caches of major search engines

- Check for User-Agent-based content differences

- Perform Web Application Fingerprinting

- Identify technologies used, user roles, app entry points

- Identify client-side code, multiple versions/channels

- Identify co-hosted and related applications

- Identify all hostnames and ports

- Identify third-party hosted content

- Identify Debug parameters

Configuration Management

- Check common admin URLs, old/backup files

- Check HTTP methods, XST

- Test file extension handling

- Test security HTTP headers (CSP, X-Frame, HSTS)

- Test for policy files and non-production data

- Check client-side sensitive data (API keys, creds)

Secure Transmission

- Check SSL version, algorithm, key length

- Validate digital certificate

- Ensure credentials and login forms use HTTPS

- Verify session tokens over HTTPS

- Confirm HSTS is in use

Authentication

- Test user enumeration, bypass, bruteforce protection

- Check password rules, remember me, autocomplete

- Test password reset, change, CAPTCHA, MFA

- Test logout, cache management, default logins

- Check for auth history, account lockout notifications

- Check for SSO consistency

Session Management

- Identify session management mechanism

- Check cookie flags, scope, duration

- Test session termination (timeout, logout, max lifetime)

- Verify session randomness, token renewal

- Test multiple simultaneous sessions

- Test for CSRF, clickjacking, puzzling

Authorization

- Test for path traversal, schema bypass

- Test for vertical and horizontal privilege issues

- Test for missing authorization

Data Validation

- Test XSS (reflected, stored, DOM), HTML Injection

- Test various injections (SQL, LDAP, XML, XXE, SSI, XPath, XQuery, IMAP, SMTP)

- Test for command/code/overflow/format string

- Test HTTP splitting/smuggling, verb tampering, open redirects

- Test for LFI, RFI, NoSQL, parameter pollution, auto-binding, mass assignment

- Compare client/server-side validation

Denial of Service

- Test anti-automation, account lockout, protocol-based DoS, wildcard DoS

Business Logic

- Test for feature misuse, trust, integrity, segregation of duties

Cryptography

- Ensure encryption where required

- Check algorithms, salting, randomness

Risky Functionality - File Uploads

- Validate file types, size, frequency, and count

- Verify content-type match, AV scanning, sanitisation

- Check access control and hostname segregation

Risky Functionality - Card Payment

- Scan for known vulns, defaults, config issues

- Ensure secure storage, transport, error handling

- Test CVSS > 4.0 issues, CSRF, Auth/AuthZ

HTML5 Specifics

- Test Web Messaging, Web Storage SQLi

- Verify CORS and Offline Web App configs