

[Get started](#)[Open in app](#)

# Chintan Gurjar

[Follow](#)

49 Followers

[About](#)

## Professional Web Application Pentest Checklist

[Chintan Gurjar](#) · Jul 29, 2020

I have started giving back to the community, and hence I have published my own professional web application pentest checklist with the world.

Please make the most of it and let's together secure the world.

The latest checklist is here —

[https://www.linkedin.com/posts/chintangurjar\\_checklist-activity-6695581576262242304-hyLY](https://www.linkedin.com/posts/chintangurjar_checklist-activity-6695581576262242304-hyLY)

Kindly keep visiting the link as this checklist is in-progress and will continue to update.

<div><div>1. Fingerprinting Application</div><div>ALL TASKSOPEN TASKSCOMPLETED TASKS</div><div><div><input type="checkbox"/> Identify known vulnerabilities in web/app server</div><div><input type="checkbox"/> Generate site structure</div><div><input type="checkbox"/> Identify underlying web technology</div><div><input type="checkbox"/> Uncover HTTP services running on ports other than 80 and 443</div><div><input type="checkbox"/> Brute-force subdomains with online tools and github scripts</div><div><input type="checkbox"/> Identify firewall</div><div><input type="checkbox"/> Find sensitive keywords in HTML, source such as admin, http, todo, redirect, etc.</div></div><div>+ Add new task</div></div>	<div><div>2. Network Testing</div><div>ALL TASKSOPEN TASKSCOMPLETED TASKS</div><div><div><input type="checkbox"/> Test for PING (ICMP echo packets)</div><div><input type="checkbox"/> Test for ZONE transfer</div><div><input type="checkbox"/> Find all services running using NMAP</div><div><input type="checkbox"/> Perform Nessus scan</div><div><input type="checkbox"/> Test all common UDP ports and related issues</div><div><input type="checkbox"/> Test SSL/TLS using Qualys</div></div><div>+ Add new task</div></div>	<div><div>3. Session Management Testing</div><div>ALL TASKSOPEN TASKSCOMPLETED TASKS</div><div><div><input type="checkbox"/> Identify actual session cookie out of bulk cookies</div><div><input type="checkbox"/> Decode cookies using standard algorithms such as base64, hex, etc.</div><div><input type="checkbox"/> Modify 1 character in cookie token and resubmit, check whether session still exists or not</div><div><input type="checkbox"/> Token leakage via Referer header - Untrusted 3rd party</div><div><input type="checkbox"/> Check session cookie expiration time</div><div><input type="checkbox"/> Identify cookie domain scope</div><div><input type="checkbox"/> Check flags HTTPOnly, Secure flag and same-site</div><div><input type="checkbox"/> Check before and after session cookie values</div><div><input type="checkbox"/> Reply the session cookie from a different public IP address and check if app maintai...</div><div><input type="checkbox"/> Check concurrent login through different IP</div><div><input type="checkbox"/> Check if any user pertaining information stored in cookie value or not, if yes tamper f...</div></div><div>+ Add new task</div></div>
<div><div>4. Registration Feature Testing</div><div>ALL TASKSOPEN TASKSCOMPLETED TASKS</div><div><div><input type="checkbox"/> Check for duplicate registration with same email id for account takeover</div><div><input type="checkbox"/> Check for weak password policy</div><div><input type="checkbox"/> Check for stored username as a part of welcome message post authentication and r...</div><div><input type="checkbox"/> Check for insufficient email verification process</div><div><input type="checkbox"/> Weak registration implementation - Allows disposable email addresses</div></div><div>+ Add new task</div></div>	<div><div>5. Login Feature Testing</div><div>ALL TASKSOPEN TASKSCOMPLETED TASKS</div><div><div><input type="checkbox"/> Check username enumeration</div><div><input type="checkbox"/> Bypass login panel with common login SQL injection payloads using BurpSuite Intruder</div><div><input type="checkbox"/> Try accessing resources without authentication</div><div><input type="checkbox"/> Check if user creds are sent over http</div><div><input type="checkbox"/> Check if user creds can forcefully be submitted over http while http and https both are ...</div><div><input type="checkbox"/> Check account logout threshold value</div><div><input type="checkbox"/> Create custom password wordlist and try bruteforce</div><div><input type="checkbox"/> Test OAuth functionality</div><div><input type="checkbox"/> Test OAuth functionality for open redirect</div></div><div>+ Add new task</div></div>	<div><div>6. Error Codes Testing</div><div>ALL TASKSOPEN TASKSCOMPLETED TASKS</div><div><div><input type="checkbox"/> Try accessing custom pages after root directory such as youname.php, youname.a...</div><div><input type="checkbox"/> Add multiple parameters in same post get request using different value and generate...</div><div><input type="checkbox"/> Add [ ], and [ ] in cookie values and parameter values to create errors</div><div><input type="checkbox"/> Try to generate unusual error code by giving input as ~youname% at the end of w...</div><div><input type="checkbox"/> Use fuzzing technique to create errors and determine any information leakage</div></div><div>+ Add new task</div></div>

[Get started](#)[Open in app](#)

+ Add new task

12. Cross-Site Scripting Testing

ALL TASKS OPEN TASKS COMPLETED TASKS

☐ Test what's being sanitised and what not

☐ Try XSS using XSSStrike tool by Somdev Sangwan

☐ Upload file using ">img src=x onerror=alert(document.domain)> txt

☐ Try all variations of IMG SRC onerror payloads

☐ 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...

☐ If " are filtered then use this payload ->img src=onerror=confirm(/site/)>

☐ Upload a javascript using Image file - use gifhide tool

☐ Unusual way to execute your JS payload is to change method from POST to GET. It b...

☐ Tag attribute value - 1. Input landed - <input type="text" name="state" value="INPUT\_...

☐ Syntax Encoding payload - %3script%3ealert(document.cookie)%3script%3e

☐ ASP.NET IE9 Filter evasion - HTML entities - &lt;%tag style="test:expression(alert(1...

☐ ASP.NET IE9 Filter evasion - HTML entities - %tag style="test:expression(alert(123))"

☐ Try base64 payload

☐ If the logout button just performs the redirection then use old classic XSS payload

☐ Try Polygot payload

+ Add new task

10. Product Purchase Testing

ALL TASKS OPEN TASKS COMPLETED TASKS

☐ 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 ...

☐ Check if security questions are asked? a. How many guesses allowed? -> Lockout ...

☐ Add only spaces in new password and confirmed password. Then Hit enter and see ...

☐ Does it display old password on the same page after completion of forget password f...

☐ 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

+ Add new task

11. Flight/Hotel/Railway Booking Testing

ALL TASKS OPEN TASKS COMPLETED TASKS

☐ Booking details - View/Manage other user's booking details.

☐ Booking details - Check reservation status for other users/behalf of other users.

☐ Ticket/Vouchers - View other users vouchers/tickets from PRINT option

☐ Ticket/Vouchers - Check if sensitive data is passed in GET request

☐ Ticket/Vouchers - If e-ticket/voucher is sent on email then check for the email floodin ...

☐ Refund - View other user's refund status.

☐ Refund - Refund more money than the intended one by parameter manipulation.

☐ Refund - If refund tracking is allowed then gain other user's refund tracking status.

☐ Cancellation - Gain higher cancellation amount with parameter modifying for amount ...

☐ Booking - Do 1st person booking and add 5 more other persons in same prize

☐ Booking - Hotel - Book normal room - Select Deluxe room in the same prize

+ Add new task

15. ASP.NET Application Specific Testing (Web and Thick client)

ALL TASKS OPEN TASKS COMPLETED TASKS

[Cybersecurity](#)

[Informationsecurity](#)

[Infosec](#)

[Bugbounty](#)

[Hacking](#)

[About](#) [Help](#) [Legal](#)

[Get the Medium app](#)