Web Application Penetration Test Checklist | Part – 01

In this article I am going to share a checklist which you can use when you are doing a penetration test on a website, you can also use this list as a reference in bug bounties. This is beginner’s friendly list, so they can look it for reference.

Before stating the list I want to make something clear, that before you start using this list for finding bugs/vulnerabilities make sure that you have already completed the first step which is “Reconnaissance”. Otherwise you will find it hard to find bug/vulnerabilities.

**You are not genius!** Remember this thing, so if you don’t understand something just Google about it and so some research, I also don’t know everything and there could be things that I have missed, so don’t worry and keep learning.

**General things to do**

1. Create 2 accounts on the same website if it has login functionality. You can use this [extension]( <https://addons.mozilla.org/en-US/firefox/addon/multi-account-containers/>) to use same browser for creating different accounts on the same website.
2. Try directory forcing using tools like “Dirsearch”, “FeroBuster”, “Ffuf”, might be possible some directory may reveal sensitive information.

**Login page**

1. Session expiration
2. Improper session validation
3. OAuth bypass (it includes features like login with Google, Microsoft, Instagram or any)
   * OAuth token stealing
   * Authentication bypass
   * Privilege escalation
   * SQLi

**Registration page**

1. XML file upload using SVG (if website asks for documents upload or profile upload then you can try this)
2. Bypassing limitation on file types to upload (if they just allow jpg, png then try to upload .php or .py)
3. Bypassing mobile or email verification
4. Brute forcing OTP sent
5. Try inserting XSS payload whenever possible (like If you can enter payload in first name/last name/address etc text box makes sure to enter because sometimes it may reflects somewhere else or maybe it’s stored XSS).

**Forgot password page**

1. Password reset poisoning (kind of similar way we do host header injection)
2. Reset token/link expiring (maybe they pay)
3. Reset token leaks (this can happen when some website interacts to third party services at that point of time maybe password reset token is sent via referrer part and maybe it can leak)
4. Check for sub-domain takeover.
5. Check for older version of service is being used by your target and if they so try to find existing exploit for the target.

So this was all about some basic things to check while doing penetration test on a website or in a bug bounty program. Hope you liked it and learned something new from it.

If you have any doubt, question, quires related to this topic or just want to share something with me, than please feel free to contact me.