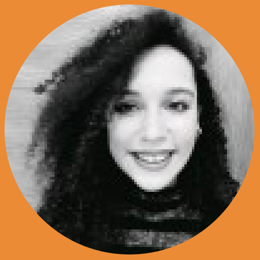
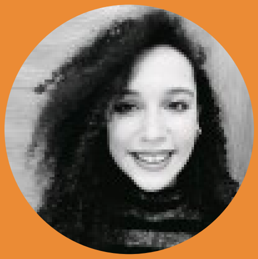


Burcu Yarar @brcyrr

Roadmap Suggestion of the Week

Web Application Pentesting Roadmap

Next →



Burcu Yarar @brcyrr

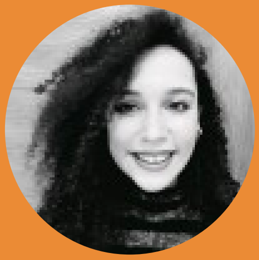
This roadmap includes sample answers to the following questions.

1. Which source should **you read?**

2. Which cheat sheet should **you use?**

3. Which vulnerable lab environment should **you practice?**

Next →

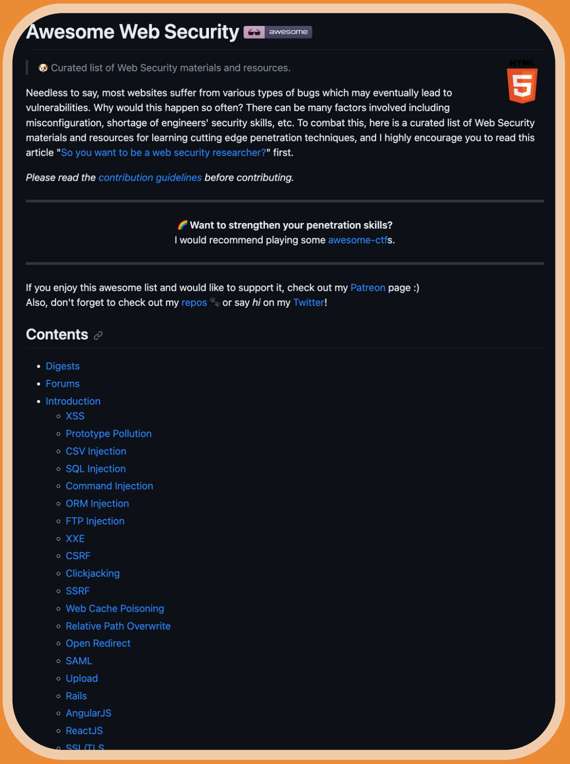


Burcu Yarar @brcyrr

Which resource should **you read?**

Awesome Web Security

Resource Link



Awesome Web Security 🕶 awesome

> 🐶 Curated list of Web Security materials and resources.

Needless to say, most websites suffer from various types of bugs which may eventually lead to vulnerabilities. Why would this happen so often? There can be many factors involved including misconfiguration, shortage of engineers' security skills, etc. To combat this, here is a curated list of Web Security materials and resources for learning cutting edge penetration techniques, and I highly encourage you to read this article "So you want to be a web security researcher?" first.

Please read the contribution guidelines before contributing.

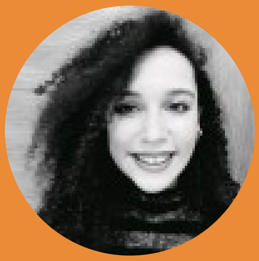
🌈 **Want to strengthen your penetration skills?**
I would recommend playing some awesome-ctfs.

If you enjoy this awesome list and would like to support it, check out my Patreon page :)
Also, don't forget to check out my repos 🐾 or say *hi* on my Twitter!

Contents

- Digests
- Forums
- Introduction
  - XSS
  - Prototype Pollution
  - CSV Injection
  - SQL Injection
  - Command Injection
  - ORM Injection
  - FTP Injection
  - XXE
  - CSRF
  - Clickjacking
  - SSRF
  - Web Cache Poisoning
  - Relative Path Overwrite
  - Open Redirect
  - SAML
  - Upload
  - Rails
  - AngularJS
  - ReactJS
  - SSL/TLS

Next →

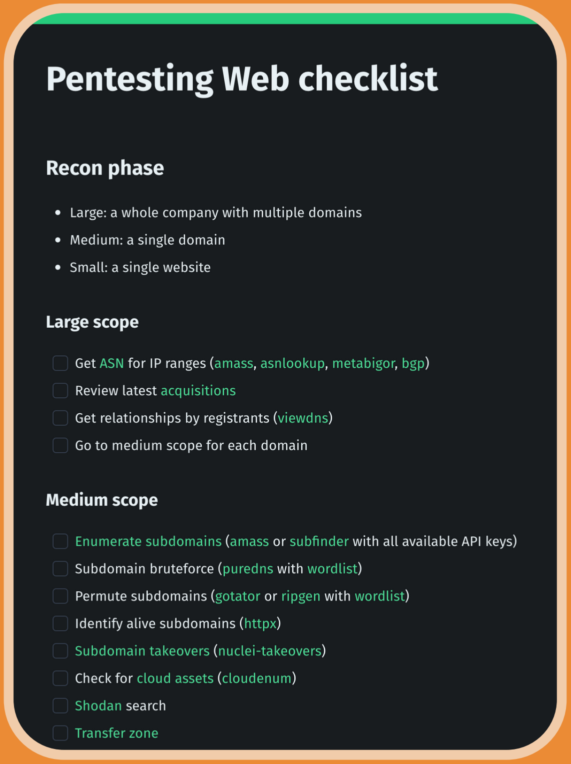


Burcu Yarar @brcyrr

Which cheat sheet should **you use?**

Pentesting Web checklist

Resource Link



Pentesting Web checklist

Recon phase

- Large: a whole company with multiple domains
- Medium: a single domain
- Small: a single website

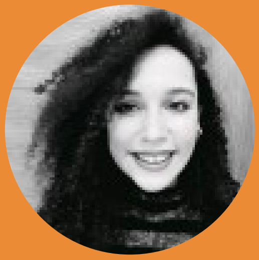
Large scope

□ Get ASN for IP ranges (amass, asnlookup, metabigor, bgp)
□ Review latest acquisitions
□ Get relationships by registrants (viewdns)
□ Go to medium scope for each domain

Medium scope

□ Enumerate subdomains (amass or subfinder with all available API keys)
□ Subdomain bruteforce (puredns with wordlist)
□ Permute subdomains (gotator or ripgen with wordlist)
□ Identify alive subdomains (httpx)
□ Subdomain takeovers (nuclei-takeovers)
□ Check for cloud assets (cloudenum)
□ Shodan search
□ Transfer zone

Next →

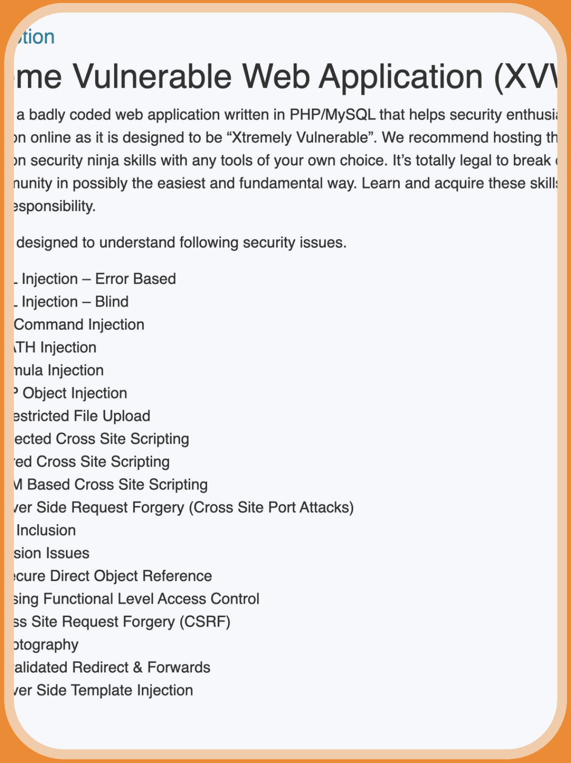


Burcu Yarar @brcyrr

Which vulnerable lab environment should **you practice?**

Xtreme Vulnerable Web Application (XVWA)

Resource Link



tion

me Vulnerable Web Application (XV

a badly coded web application written in PHP/MySQL that helps security enthusi
n online as it is designed to be "Xtremely Vulnerable". We recommend hosting th
n security ninja skills with any tools of your own choice. It's totally legal to break
nunity in possibly the easiest and fundamental way. Learn and acquire these skill
esponsibility.

designed to understand following security issues.

Injection – Error Based
Injection – Blind
Command Injection
TH Injection
nula Injection
Object Injection
estricted File Upload
ected Cross Site Scripting
ed Cross Site Scripting
I Based Cross Site Scripting
ver Side Request Forgery (Cross Site Port Attacks)
Inclusion
sion Issues
cure Direct Object Reference
sing Functional Level Access Control
ss Site Request Forgery (CSRF)
otography
alidated Redirect & Forwards
ver Side Template Injection

End ★