



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 →

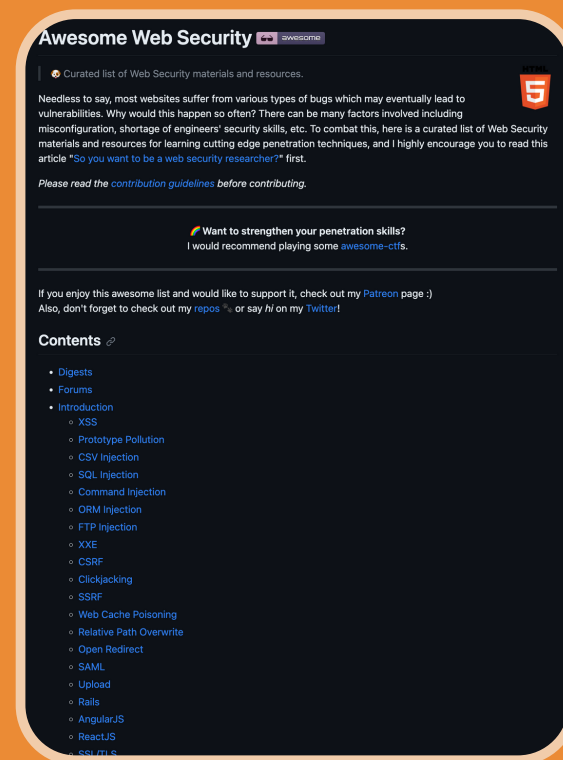


Burcu Yarar @brcyrr

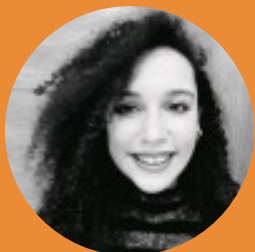
Which resource should **you** read?

Awesome Web Security

Resource Link



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

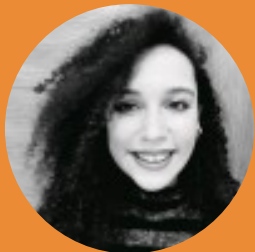
Large scope

- ☐ 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

Xtreme Vulnerable Web Application (XVWA)

a badly coded web application written in PHP/MySQL that helps security enthusiasts practice their skills online as it is designed to be "Xtremely Vulnerable". We recommend hosting this application on your own server or using a cloud provider. We recommend practicing your security ninja skills with any tools of your own choice. It's totally legal to break into a system in possibly the easiest and fundamental way. Learn and acquire these skills responsibly.

designed to understand following security issues.

- SQL Injection – Error Based
- SQL Injection – Blind
- Command Injection
- HTTP Injection
- LDAP Injection
- PHP Object Injection
- Restricted File Upload
- Reflected Cross Site Scripting
- Stored Cross Site Scripting
- LDAP Based Cross Site Scripting
- Cross Site Request Forgery (Cross Site Request Attacks)
- Inclusion
- Session Issues
- Secure Direct Object Reference
- Missing Functional Level Access Control
- Cross Site Request Forgery (CSRF)
- Photography
- Validated Redirect & Forwards
- Cross Site Template Injection

End ★