Getting started with Web app security

Tools to use for pentesting web applications –

• Proxy tool – BurpSuite, MITMProxy, Charles etc.

• Browser features - Chrome Developer tools, Firebug etc.

• Security Scanners – w3af, nikto, arachni, OWASP Zap etc.

• Individual tools for various vulnerabilities

BurpSuite 101

• Most popular proxy tool among security professionals

• Easy to use

• Contains a number of tools including proxy, intruder, repeater, decoder and additional plugins

• Can write additional scripts for Burp and use it

• Alternatives – MITMproxy, Fiddler, Charles etc.

Setting up BurpSuite for our lab

• Set the browser's proxy to 127.0.0.1 and port 8080

• Make sure you intercept request and response

• Launch up Burp

• Start listening on port 8080

Getting started with BurpSuite

• Once you have the traffic intercepted, you can modify and then send it to the web application

• Ability to modify both request and response

- Repeater functionality

```
Thanks & Regards
Harshad Shah
Founder & CEO, Hacker Associate
```