**Bug Bounty**

* **Attacking Web Servers**
  + **File inclusion**
  + **Command injection**
  + **Remote code Execution**
  + **Unrestricted upload**
  + **Server-side request forgery**
  + **Server-Side Template Injection**
  + **Insecure Deserialization**
  + **XSLT Injection**
  + **SSI Vulnerability**
* **Attacking Data stores**
  + **SQL injection**
    - **NoSQL injection**
  + **Xml injections**
    - **xpath injection**
    - **The XML External Entity injection (XXE)**
    - **entity expansion attack**
    - **soap injecting**
  + **Ldap injection**
* **Attacking Users**
  + **Html injection**
  + **Cross site scripting**
  + **Cross site request forgery**
  + **HTTP parameter injection**
    - **Http parameter pollution**
    - **Open Redirect**
  + **Click jacking**
  + **Insecure CORS**
  + **Web sockets Attacks**
  + **Dom Attacks**
* **Information Disclosure**
* **Attacking Authentication**
  + **Authentication Methods**
  + **HTTP Authentication**
  + **2 factor Authentication Bypass**
  + **Insecure captcha**
  + **Oauth attacks**
  + **Saml Attacks**
* **Attacking Access control & Security misconfigurations**
  + **Horizontal Access control** 
    - **IDOR**
  + **Vertical Access Control**
  + **Context Based Access Control**
* **Other attacks**
  + **Subdomain takeover**
  + **Php Type juggling**
  + **Insecure Deserialization**
  + **Host Header attack**
  + **Cache poisoning attack**
  + **CRLF Injection**
  + **HTTP Request Smuggling**
  + **SMTP injection**
  + **Missing SPF record**
  + **Php remote xdebug vulnerability**
  + **Using components with known vulnerabilities**
  + **Race conditions**
  + **HTTP verb tempering**
  + **Exploiting Put Method**
  + **Insufficient logging and Monitoring**
  + **CMS Exploitation**
* **Bug bounty methodology**
* **Concepts and Notes**

**-------------------------------------------------------------------------**