Web Application Hacking and Security (WAHS)

Exam Blueprint v1
### Web Application Hacking and Security (WAHS)

#### Exam Blueprint

(Version 1)

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Domains</th>
<th>Sub-domains</th>
<th>Weightage</th>
</tr>
</thead>
</table>
| 1      | Broken Access Control             | ▪ Privilege escalation  
▪ Insecure direct object references  
▪ Parameter tampering  
▪ API abuse  
▪ Metadata manipulation  
▪ CORS misconfiguration | 20%       |
| 2      | Cryptographic Failures            | ▪ Weak cryptographic algorithms or protocols  
▪ Weak crypto keys  
▪ HTTP headers security directives  
▪ Insufficient entropy  
▪ Deprecated hash functions  
▪ Deprecated cryptographic padding methods | 16%       |
| 3      | Injection                         | ▪ Code injection  
▪ CRLF injection  
▪ Cross-site Scripting (XSS)  
▪ Email Header Injection  
▪ Host Header Injection  
▪ LDAP Injection  
▪ OS Command Injection  
▪ SQL Injection (SQLi)  
▪ XPath injection | 12%       |
<p>| 4      | Insecure Design                   | ▪ Notable Common Weakness Enumerations | 16%       |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
|   | ▪ Error Message Containing Sensitive Information  
  ▪ Unprotected Storage of Credentials  
  ▪ Trust Boundary Violation  
  ▪ Insufficiently Protected Credentials  
  ▪ Software and Data Integrity Failures  
  ▪ Security Logging and Monitoring Failures  
  ▪ Server-Side Request Forgery |   |   |
| 5 | **Security Misconfiguration** | ▪ Improperly configured permissions  
  ▪ Unnecessary features  
  ▪ Default accounts  
  ▪ Poor error handling | 12% |
| 6 | **Vulnerable and Outdated Components** | ▪ Unmaintained Third-Party Components  
  ▪ Vulnerable third-party libraries or frameworks | 4% |
| 7 | **Identification and Authentication Failures** | ▪ Improper Validation of Certificate  
  ▪ Session Fixation  
  ▪ Improper Authentication | 20% |