**Basic System TOOLS**

1. **Kali Linux Installation**
2. **Introduction to CIA**
3. **Nmap**
4. **BurpSuite**
5. **Metasploit**
6. **Wordlists**
7. **Wpscan**
8. **Gobuster**
9. **Wfuzz/ffuf**
10. **Hakrawler**
11. **Shell**
12. **Security Headers - HTTP**

**WEB APPLICATION BUGS LISTS**

1. **SQL injection**
2. **XSS**
3. **CSRF**
4. **Clickjacking**
5. **DOM-based**
6. **CORS**
7. **XXE**
8. **SSRF**
9. **Request smuggling**
10. **Command injection**
11. **Server-side template injection**
12. **Insecure deserialization**
13. **Directory traversal**
14. **Access control**
15. **Authentication**
16. **OAuth authentication**
17. **Business logic vulnerabilities**
18. **Web cache poisoning**
19. **HTTP Host header attacks**
20. **WebSockets**
21. **Information disclosure**
22. **File upload vulnerabilities**
23. **JWT attacks**
24. **Prototype pollution**

**Machine Lab Lists**

1. **Union- Hack the Box**
2. **Holiday (sql,xss)- Hack the Box**
3. **PortSwigger Lab- CSRF**
4. **PortSwigger Lab – Click Jacking**
5. **CrossFit2 - Hack The Box**
6. **Por tSwigger Lab- Cors**
7. **BountyHunter – Hack the Box**
8. **Forge – Hack the Box**
9. **Sink – Hack the Box**
10. **Validation – (ci) Hack the Box**
11. **Doctor – (ssti) Hack the Box**
12. **PortSwigger Lab – Insecure deserialization**
13. **Unicode – Hack the Box**
14. **Control – Hack the Box**
15. **PortSwigger Lab – Authentication**
16. **PortSwigger Lab - OAuth**
17. **PortSwigger Lab – Business Logic**
18. **Forgot – Hack the box**
19. **Forgot – Hack the box**
20. **PortSwigger Lab – WebSocket**
21. **PortSwigger Lab – Access Control**
22. **Magic – Hack the Box**
23. **Unicode – Hack the Box**
24. **Self- Work**

**Owasp Top 10**

**A01:2021-Broken Access Control**

**A02:2021-Cryptographic Failures**

**A03:2021-Injection**

**A04:2021-Insecure Design**

**A05:2021-Security Misconfiguration**

**A06:2021-Vulnerable and Outdated Components**

**A07:2021-Identification and Authentication Failures**

**A08:2021-Software and Data Integrity Failures**

**A09:2021-Security Logging and Monitoring Failures**

**A10:2021-Server-Side Request Forgery**

**## Best Website list**

**https://cheatsheetseries.owasp.org/cheatsheets/HTTP\_Headers\_Cheat\_Sheet.html**

**Hack the Box –Box List**

|  |  |  |
| --- | --- | --- |
| Squashed  Photobomb  Shoppy  RedPanda  Trick  OpenSource  GoodGames  RouterSpace  SteamCloud  Paper  Pandora  Backdoor  Nunchucks  Secret  Antique  Validation  Horizontall  Previse  BountyHunter  Cap  Knife  Armageddon  ScriptKiddie  Delivery  Laboratory  Academy  Doctor  Tabby  Blunder  Admirer  Traceback  OpenAdmin  Traverxec  Postman  Writeup  SwagShop  FriendZone  Help  Blocky | Forgot  Awkward  Ambassador  Health  Shared  Faculty  Noter  Ransom  Retired  Catch  Undetected  Flustered  Meta  LogForge  Timing  Union  Unicode  Shibboleth  Bolt  Gobox  Forge  Writer  Seal  Schooled  TheNotebook  Time  Cache  Magic  Book  AI  Mango  Jarvis  Luke  Unattended  Lightweight  Vault  Poison  Node  Nineveh  Europa  Haircut  October  Cronos | RainyDay  Moderators  Extension  Carpediem  Seventeen  Talkative  Pressed  AdmirerToo  Spooktrol  Pikaboo  Static  Spider  Monitors  Compromised  Joker |