Web Application Penetration Testing

Phase 1 – History

1. History of Internet - https://www.youtube.com/watch?v=9hIQjrMHTv4

Phase 2 – Web and Server Technology

2. Basic concepts of web applications, how they work and the HTTP protocol - https://www.youtube.com/watch?v=RsQ1tFLwldY&t=7s
3. HTML basics part 1 - https://www.youtube.com/watch?v=p6fRBGI_BY0
4. HTML basics part 2 - https://www.youtube.com/watch?v=Zs6lzuBVK2w
5. Difference between static and dynamic website - https://www.youtube.com/watch?v=hlg6q6OFoxQ
6. HTTP protocol Understanding - https://www.youtube.com/watch?v=JFZMyhRTVt0
7. Parts of HTTP Request -https://www.youtube.com/watch?v=pHFWGN-upGM
8. Parts of HTTP Response - https://www.youtube.com/watch?v=c9sMNc2PrMU
9. Various HTTP Methods - https://www.youtube.com/watch?v=PO7D20HsFsY
10. Understanding URLS - https://www.youtube.com/watch?v=5Jr-_Za5yQM
11. Intro to REST - https://www.youtube.com/watch?v=YCcAE2SCQ6k
12. HTTP Request & Response Headers - https://www.youtube.com/watch?v=vAuZwirKjWs
13. What is a cookie - https://www.youtube.com/watch?v=I01XMRo2ESg
14. HTTP Status codes - https://www.youtube.com/watch?v=VLH3FMQ5BIQ
15. HTTP Proxy - https://www.youtube.com/watch?v=qU0PVSJCKcs
16. Authentication with HTTP - https://www.youtube.com/watch?v=GxiFXUFKo1M
17. HTTP basic and digest authentication - https://www.youtube.com/watch?v=GOnhCbDhMzk
18. What is “Server-Side” - https://www.youtube.com/watch?v=JnCLmLO9LhA
19. Server and client side with example - https://www.youtube.com/watch?v=DcBB2Fp8WNI
20. What is a session - https://www.youtube.com/watch?v=WV4DJ6b0jhg&t=202s
21. Introduction to UTF-8 and Unicode - https://www.youtube.com/watch?v=sqPTR_v4qFA
22. URL encoding - https://www.youtube.com/watch?v=Z3udiqgW1VA
23. HTML encoding - https://www.youtube.com/watch?v=IiAfCLWpgII&t=109s
24. Base64 encoding - https://www.youtube.com/watch?v=8qkxeZmKmOY
25. Hex encoding & ASCII - https://www.youtube.com/watch?v=WW2SaCMnHdU

Phase 3 – Setting up the lab with BurpSuite and bWAPP

MANISH AGRAWAL

26. Setup lab with bWAPP - https://www.youtube.com/watch?v=dwtUn3giwTk&index=1&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV
27. Set up Burp Suite - https://www.youtube.com/watch?v=hQsT4rSa_v0&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV&index=2
28. Configure Firefox and add certificate - https://www.youtube.com/watch?v=hfsdJ69GSV4&index=3&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV
29. Mapping and scoping website - https://www.youtube.com/watch?v=H-_iVteMDRo&index=4&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV
30. Spidering - https://www.youtube.com/watch?v=97uMUQGIe14&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV&index=5
31. Active and passive scanning - https://www.youtube.com/watch?v=1Mjom6AcFyU&index=6&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV
32. Scanner options and demo - https://www.youtube.com/watch?v=gANi4Kt7-ek&index=7&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV
33. Introduction to password security - https://www.youtube.com/watch?v=FwcUhcLO9iM&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV&index=8
34. Intruder - https://www.youtube.com/watch?v=wtMg9oEMTa8&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV&index=9
35. Intruder attack types - https://www.youtube.com/watch?v=N5ndYPwddkQ&index=10&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV
36. Payload settings - https://www.youtube.com/watch?v=5GpdlbtL-1Q&index=11&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV
37. Intruder settings - https://www.youtube.com/watch?v=B_Mu7jmOYnU&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV&index=12

ÆTHER SECURITY LAB

38. No.1 Penetration testing tool - https://www.youtube.com/watch?v=AVzC7ETqpDo&list=PLq9n8iqQJFDrwFe9AEDBlR1uSHEN7egQA&index=1
39. Environment Setup - https://www.youtube.com/watch?v=yqnUOdr0eVk&index=2&list=PLq9n8iqQJFDrwFe9AEDBlR1uSHEN7egQA
40. General concept - https://www.youtube.com/watch?v=udl4oqr_ylM&list=PLq9n8iqQJFDrwFe9AEDBlR1uSHEN7egQA&index=3
41. Proxy module - https://www.youtube.com/watch?v=PDTwYFkjQBE&list=PLq9n8iqQJFDrwFe9AEDBlR1uSHEN7egQA&index=4
42. Repeater module - https://www.youtube.com/watch?v=9Zh_7s5csCc&list=PLq9n8iqQJFDrwFe9AEDBlR1uSHEN7egQA&index=5
43. Target and spider module - https://www.youtube.com/watch?v=dCKPZUSOlr8&list=PLq9n8iqQJFDrwFe9AEDBlR1uSHEN7egQA&index=6
44. Sequencer and scanner module - https://www.youtube.com/watch?v=G-v581pXerE&list=PLq9n8iqQJFDrwFe9AEDBlR1uSHEN7egQA&index=7

Phase 4 – Mapping the application and attack surface

45. Spidering - https://www.youtube.com/watch?v=97uMUQGIe14&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV&index=5
46. Mapping application using robots.txt - https://www.youtube.com/watch?v=akuzgZ75zrk
47. Discover hidden contents using dirbuster - https://www.youtube.com/watch?v=--nu9Jq07gA
48. Dirbuster in detail - https://www.youtube.com/watch?v=2tOQC68hAcQ
49. Discover hidden directories and files with intruder - https://www.youtube.com/watch?v=4Fz9mJeMNkI
50. Directory bruteforcing 1 - https://www.youtube.com/watch?v=ch2onB_LFoI
51. Directory bruteforcing 2 - https://www.youtube.com/watch?v=ASMW_oLbyIg
52. Identify application entry points - https://www.youtube.com/watch?v=IgJWPZ2OKO8&t=34s
53. Identify application entry points - https://www.owasp.org/index.php/Identify_application_entry_points_(OTG-INFO-006)
54. Identify client and server technology - https://www.youtube.com/watch?v=B8jN_iWjtyM

55. Identify server technology using banner grabbing (telnet) - https://www.youtube.com/watch?v=O67M-U2UOAg
56. Identify server technology using httprecon - https://www.youtube.com/watch?v=xBBHtS-dwsM
57. Pentesting with Google dorks Introduction - https://www.youtube.com/watch?v=NmdrKFwAw9U
58. Fingerprinting web server - https://www.youtube.com/watch?v=tw2VdG0t5kc&list=PLxLRoXCDIalcRS5Nb1I_HM_OzS10E6lqp&index=10
59. Use Nmap for fingerprinting web server - https://www.youtube.com/watch?v=VQV-y_-AN80
60. Review webs servers metafiles for information leakage - https://www.youtube.com/watch?v=sds3Zotf_ZY
61. Enumerate applications on web server - https://www.youtube.com/watch?v=lfhvvTLN60E
62. Identify application entry points - https://www.youtube.com/watch?v=97uMUQGIe14&list=PLDeogY2Qr-tGR2NL2X1AR5Zz9t1iaWwlM
63. Map execution path through application - https://www.youtube.com/watch?v=0I0NPiyo9UI
64. Fingerprint web application frameworks - https://www.youtube.com/watch?v=ASzG0kBoE4c

Phase 5 – Understanding and exploiting OWASP top 10 vulnerabilities

65. A closer look at all owasp top 10 vulnerabilities - https://www.youtube.com/watch?v=avFR_Af0KGk

IBM

66. Injection - https://www.youtube.com/watch?v=02mLrFVzIYU&index=1&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d
67. Broken authentication and session management - https://www.youtube.com/watch?v=iX49fqZ8HGA&index=2&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d
68. Cross-site scripting - https://www.youtube.com/watch?v=x6I5fCupLLU&index=3&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d
69. Insecure direct object reference - https://www.youtube.com/watch?v=-iCyp9Qz3CI&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d&index=4
70. Security misconfiguration - https://www.youtube.com/watch?v=cIplXL8idyo&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d&index=5
71. Sensitive data exposure - https://www.youtube.com/watch?v=rYlzTQlF8Ws&index=6&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d
72. Missing functional level access controls - https://www.youtube.com/watch?v=VMv_gyCNGpk&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d&index=7
73. Cross-site request forgery - https://www.youtube.com/watch?v=_xSFm3KGxh0&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d&index=8
74. Using components with known vulnerabilities - https://www.youtube.com/watch?v=bhJmVBJ-F-4&index=9&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d
75. Unvalidated redirects and forwards - https://www.youtube.com/watch?v=L6bYKiLtSL8&index=10&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d

F5 CENTRAL

76. Injection - https://www.youtube.com/watch?v=rWHvp7rUka8&index=1&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD
77. Broken authentication and session management - https://www.youtube.com/watch?v=mruO75ONWy8&index=2&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD
78. Insecure deserialisation - https://www.youtube.com/watch?v=nkTBwbnfesQ&index=8&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD
79. Sensitive data exposure - https://www.youtube.com/watch?v=2RKbacrkUBU&index=3&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD
80. Broken access control - https://www.youtube.com/watch?v=P38at6Tp8Ms&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD&index=5
81. Insufficient logging and monitoring - https://www.youtube.com/watch?v=IFF3tkUOF5E&index=10&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD

82. XML external entities - https://www.youtube.com/watch?v=g2ey7ry8_CQ&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD&index=4
83. Using components with known vulnerabilities - https://www.youtube.com/watch?v=IGsNYVDKRV0&index=9&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD
84. Cross-site scripting - https://www.youtube.com/watch?v=IuzU4y-UjLw&index=7&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD
85. Security misconfiguration - https://www.youtube.com/watch?v=JuGSUMtKTPU&index=6&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD

LUKE BRINER

86. Injection explained - https://www.youtube.com/watch?v=1qMggPJpRXM&index=1&list=PLpNYlUeSK_rkrrBox-xvSkm5lgaDqKa0X
87. Broken authentication and session management - https://www.youtube.com/watch?v=fKnG15BL4AY&list=PLpNYlUeSK_rkrrBox-xvSkm5lgaDqKa0X&index=2
88. Cross-site scripting - https://www.youtube.com/watch?v=ksM-xXeDUNs&index=3&list=PLpNYlUeSK_rkrrBox-xvSkm5lgaDqKa0X
89. Insecure direct object reference - https://www.youtube.com/watch?v=ZodA76-CB10&list=PLpNYlUeSK_rkrrBox-xvSkm5lgaDqKa0X&index=4
90. Security misconfiguration - https://www.youtube.com/watch?v=DfFPHKPCofY&index=5&list=PLpNYlUeSK_rkrrBox-xvSkm5lgaDqKa0X
91. Sensitive data exposure - https://www.youtube.com/watch?v=Z7hafbGDVEE&list=PLpNYlUeSK_rkrrBox-xvSkm5lgaDqKa0X&index=6
92. Missing functional level access control - https://www.youtube.com/watch?v=RGN3w831Elo&list=PLpNYlUeSK_rkrrBox-xvSkm5lgaDqKa0X&index=7
93. Cross-site request forgery - https://www.youtube.com/watch?v=XRW_US5BCxk&list=PLpNYlUeSK_rkrrBox-xvSkm5lgaDqKa0X&index=8
94. Components with known vulnerabilities - https://www.youtube.com/watch?v=pbvDW9pJdng&list=PLpNYlUeSK_rkrrBox-xvSkm5lgaDqKa0X&index=9
95. Unvalidated redirects and forwards - https://www.youtube.com/watch?v=bHTglpgC5Qg&list=PLpNYlUeSK_rkrrBox-xvSkm5lgaDqKa0X&index=10

Phase 6 – Session management testing

96. Bypass authentication using cookie manipulation - https://www.youtube.com/watch?v=mEbmturLljU
97. Cookie Security Via httponly and secure Flag - OWASP - https://www.youtube.com/watch?v=3aKA4RkAg78
98. Penetration testing Cookies basic - https://www.youtube.com/watch?v=_P7KN8T1boc
99. Session fixation 1 - https://www.youtube.com/watch?v=ucmgeHKtxaI
100. Session fixation 2 - https://www.youtube.com/watch?v=0Tu1qxysWOk
101. Session fixation 3 - https://www.youtube.com/watch?v=jxwgpWvRUSo
102. Session fixation 4 - https://www.youtube.com/watch?v=eUbtW0Z0W1g
103. CSRF - Cross site request forgery 1 - https://www.youtube.com/watch?v=m0EHlfTgGUU
104. CSRF - Cross site request forgery 2 - https://www.youtube.com/watch?v=H3iu0_ltcv4
105. CSRF - Cross site request forgery 3 - https://www.youtube.com/watch?v=1NO4I28J-0s
106. CSRF - Cross site request forgery 4 - https://www.youtube.com/watch?v=XdEJEUJ0Fr8
107. CSRF - Cross site request forgery 5 - https://www.youtube.com/watch?v=TwG0Rd0hr18
108. Session puzzling 1 - https://www.youtube.com/watch?v=YEOvmhTb8xA
109. Admin bypass using session hijacking - https://www.youtube.com/watch?v=1wp1o-1TfAc

Phase 7 – Bypassing client-side controls

110. What is hidden forms in HTML - https://www.youtube.com/watch?v=orUoGsgaYAE
111. Bypassing hidden form fields using tamper data - https://www.youtube.com/watch?v=NXkGX2sPw7I
112. Bypassing hidden form fields using Burp Suite (Purchase application) - https://www.youtube.com/watch?v=xahvJyUFTfM
113. Changing price on eCommerce website using parameter tampering - https://www.youtube.com/watch?v=A-ccNpP06Zg
114. Understanding cookie in detail - https://www.youtube.com/watch?v=_P7KN8T1boc&list=PLWPirh4EWFpESKWJmrgQwmsnTrL_K93Wi&index=18
115. Cookie tampering with tamper data- https://www.youtube.com/watch?v=NgKXm0lBecc
116. Cookie tamper part 2 - https://www.youtube.com/watch?v=dTCt_I2DWgo
117. Understanding referer header in depth using Cisco product - https://www.youtube.com/watch?v=GkQnBa3C7WI&t=35s
118. Introduction to ASP.NET viewstate - https://www.youtube.com/watch?v=L3p6Uw6SSXs
119. ASP.NET viewstate in depth - https://www.youtube.com/watch?v=Fn_08JLsrmY
120. Analyse sensitive data in ASP.NET viewstate - https://msdn.microsoft.com/en-us/library/ms972427.aspx?f=255&MSPPError=-2147217396
121. Cross-origin-resource-sharing explanation with example - https://www.youtube.com/watch?v=Ka8vG5miErk
122. CORS demo 1 - https://www.youtube.com/watch?v=wR8pjTWaEbs
123. CORS demo 2 - https://www.youtube.com/watch?v=lg31RYYG-T4
124. Security headers - https://www.youtube.com/watch?v=TNlcoYLIGFk
125. Security headers 2 - https://www.youtube.com/watch?v=ZZUvmVkkKu4

Phase 8 – Attacking authentication/login

126. Attacking login panel with bad password - Guess username password for the website and try different combinations
127. Brute-force login panel - https://www.youtube.com/watch?v=25cazx5D_vw
128. Username enumeration - https://www.youtube.com/watch?v=WCO7LnSlskE
129. Username enumeration with bruteforce password attack - https://www.youtube.com/watch?v=zf3-pYJU1c4
130. Authentication over insecure HTTP protocol - https://www.youtube.com/watch?v=ueSG7TUqoxk
131. Authentication over insecure HTTP protocol - https://www.youtube.com/watch?v=_WQe36pZ3mA
132. Forgot password vulnerability - case 1 - https://www.youtube.com/watch?v=FEUidWWnZwU
133. Forgot password vulnerability - case 2 - https://www.youtube.com/watch?v=j7-8YyYdWL4
134. Login page autocomplete feature enabled - https://www.youtube.com/watch?v=XNjUfwDmHGc&t=33s
135. Testing for weak password policy - https://www.owasp.org/index.php/Testing_for_Weak_password_policy_(OTG-AUTHN-007)
136. Insecure distribution of credentials - When you register in any website or you request for a password reset using forgot password feature, if the website sends your username and password over the email in cleartext without sending the password reset link, then it is a vulnerability.
137. Test for credentials transportation using SSL/TLS certificate - https://www.youtube.com/watch?v=21_IYz4npRs
138. Basics of MySQL - https://www.youtube.com/watch?v=yPu6qV5byu4
139. Testing browser cache - https://www.youtube.com/watch?v=2T_Xz3Humdc
140. Bypassing login panel -case 1 - https://www.youtube.com/watch?v=TSqXkkOt6oM
141. Bypass login panel - case 2 - https://www.youtube.com/watch?v=J6v_W-LFK1c

Phase 9 - Attacking access controls (IDOR, Priv esc, hidden files and directories)

Completely unprotected functionalities

142. Finding admin panel - https://www.youtube.com/watch?v=r1k2lgvK3s0
143. Finding admin panel and hidden files and directories - https://www.youtube.com/watch?v=Z0VAPbATy1A
144. Finding hidden webpages with dirbusater - https://www.youtube.com/watch?v=--nu9Jq07gA&t=5s

Insecure direct object reference

145. IDOR case 1 - https://www.youtube.com/watch?v=gci4R9Vkulc
146. IDOR case 2 - https://www.youtube.com/watch?v=4DTULwuLFS0
147. IDOR case 3 (zomato) - https://www.youtube.com/watch?v=tCJBLG5Mayo

Privilege escalation

148. What is privilege escalation - https://www.youtube.com/watch?v=80RzLSrczmc
149. Privilege escalation - Hackme bank - case 1 - https://www.youtube.com/watch?v=g3lv__87cWM
150. Privilege escalation - case 2 - https://www.youtube.com/watch?v=-i4O_hjc87Y

Phase 10 – Attacking Input validations (All injections, XSS and mics)

HTTP verb tampering

151. Introduction HTTP verb tampering - https://www.youtube.com/watch?v=Wl0PrIeAnhs
152. HTTP verb tampering demo - https://www.youtube.com/watch?v=bZlkuiUkQzE

HTTP parameter pollution

153. Introduction HTTP parameter pollution - https://www.youtube.com/watch?v=Tosp-JyWVS4
154. HTTP parameter pollution demo 1 - https://www.youtube.com/watch?v=QVZBl8yxVX0&t=11s
155. HTTP parameter pollution demo 2 - https://www.youtube.com/watch?v=YRjxdw5BAM0
156. HTTP parameter pollution demo 3 - https://www.youtube.com/watch?v=kIVefiDrWUw

XSS - Cross site scripting

157. Introduction to XSS - https://www.youtube.com/watch?v=gkMl1suyj3M

158. What is XSS - https://www.youtube.com/watch?v=cbmBDiR6WaY
159. Reflected XSS demo - https://www.youtube.com/watch?v=r79ozjCL7DA
160. XSS attack method using burpsuite - https://www.youtube.com/watch?v=OLKBZNw3OjQ
161. XSS filter bypass with Xenotix - https://www.youtube.com/watch?v=loZSdedJnqc
162. Reflected XSS filter bypass 1 - https://www.youtube.com/watch?v=m5rlLgGrOVA
163. Reflected XSS filter bypass 2 - https://www.youtube.com/watch?v=LDiXveqQ0gg
164. Reflected XSS filter bypass 3 - https://www.youtube.com/watch?v=hb_qENFUdOk
165. Reflected XSS filter bypass 4 - https://www.youtube.com/watch?v=Fg1qqkedGUk
166. Reflected XSS filter bypass 5 - https://www.youtube.com/watch?v=NImym71f3Bc
167. Reflected XSS filter bypass 6 - https://www.youtube.com/watch?v=9eGzAym2a5Q
168. Reflected XSS filter bypass 7 - https://www.youtube.com/watch?v=ObfEI84_MtM
169. Reflected XSS filter bypass 8 - https://www.youtube.com/watch?v=2c9xMe3VZ9Q
170. Reflected XSS filter bypass 9 - https://www.youtube.com/watch?v=-48zknvo7LM
171. Introduction to Stored XSS - https://www.youtube.com/watch?v=SHmQ3sQFeLE
172. Stored XSS 1 - https://www.youtube.com/watch?v=oHIl_pCahsQ
173. Stored XSS 2 - https://www.youtube.com/watch?v=dBTuWzX8hd0
174. Stored XSS 3 - https://www.youtube.com/watch?v=PFG0lkMeYDc
175. Stored XSS 4 - https://www.youtube.com/watch?v=YPUBFklUWLc
176. Stored XSS 5 - https://www.youtube.com/watch?v=x9Zx44EV-Og

SQL injection

177. Part 1 - Install SQLi lab - https://www.youtube.com/watch?v=NJ9AA1_t1Ic&index=23&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro
178. Part 2 - SQL lab series - https://www.youtube.com/watch?v=TA2h_kUqfhU&index=22&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro
179. Part 3 - SQL lab series - https://www.youtube.com/watch?v=N0zAChmZIZU&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=21
180. Part 4 - SQL lab series - https://www.youtube.com/watch?v=6pVxm5mWBVU&index=20&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro
181. Part 5 - SQL lab series - https://www.youtube.com/watch?v=0tyerVP9R98&index=19&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro
182. Part 6 - Double query injection - https://www.youtube.com/watch?v=zaRlcPbfX4M&index=18&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro
183. Part 7 - Double query injection cont.. - https://www.youtube.com/watch?v=9utdAPxmvaI&index=17&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro
184. Part 8 - Blind injection boolean based - https://www.youtube.com/watch?v=u7Z7AIR6cMI&index=16&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro
185. Part 9 - Blind injection time based - https://www.youtube.com/watch?v=gzU1YBu_838&index=15&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro
186. Part 10 - Dumping DB using outfile - https://www.youtube.com/watch?v=ADW844OA6io&index=14&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro
187. Part 11 - Post parameter injection error based - https://www.youtube.com/watch?v=6sQ23tqiTXY&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=13
188. Part 12 - POST parameter injection double query based - https://www.youtube.com/watch?v=tjFXWQY4LuA&index=12&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro
189. Part 13 - POST parameter injection blind boolean and time based - https://www.youtube.com/watch?v=411G-4nH5jE&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=10
190. Part 14 - Post parameter injection in UPDATE query - https://www.youtube.com/watch?v=2FgLcPuU7Vw&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=11

191. Part 15 - Injection in insert query - https://www.youtube.com/watch?v=ZJiPsWxXYZs&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=9
192. Part 16 - Cookie based injection - https://www.youtube.com/watch?v=-A3vVqfP8pA&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=8
193. Part 17 - Second order injection -https://www.youtube.com/watch?v=e9pbC5BxiAE&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=7
194. Part 18 - Bypassing blacklist filters - 1 - https://www.youtube.com/watch?v=5P-knuYoDdw&index=6&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro
195. Part 19 - Bypassing blacklist filters - 2 - https://www.youtube.com/watch?v=45BjuQFt55Y&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=5
196. Part 20 - Bypassing blacklist filters - 3 - https://www.youtube.com/watch?v=c-Pjb_zLpH0&index=4&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro
197. Part 21 - Bypassing WAF - https://www.youtube.com/watch?v=uRDuCXFpHXc&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=2
198. Part 22 - Bypassing WAF - Impedance mismatch - https://www.youtube.com/watch?v=ygVUebdv_Ws&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=3
199. Part 23 - Bypassing addslashes - charset mismatch - https://www.youtube.com/watch?v=du-jkS6-sbo&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=1

NoSQL injection

200. Introduction to NoSQL injection - https://www.youtube.com/watch?v=h0h37-Dwd_A
201. Introduction to SQL vs NoSQL - Difference between MySQL and MongoDB with tutorial - https://www.youtube.com/watch?v=QwevGzVu_zk
202. Abusing NoSQL databases - https://www.youtube.com/watch?v=lcO1BTNh8r8
203. Making cry - attacking NoSQL for pentesters - https://www.youtube.com/watch?v=NgsesuLpyOg

Xpath and XML injection

204. Introduction to Xpath injection - https://www.youtube.com/watch?v=2_UyM6Ea0Yk&t=3102s
205. Introduction to XML injection - https://www.youtube.com/watch?v=9ZokuRHo-eY
206. Practical 1 - bWAPP - https://www.youtube.com/watch?v=6tV8EuaHI9M
207. Practical 2 - Mutillidae - https://www.youtube.com/watch?v=fV0qsqcScI4
208. Practical 3 - webgoat - https://www.youtube.com/watch?v=5ZDSPVp1TpM
209. Hack admin panel using Xpath injection - https://www.youtube.com/watch?v=vvlyYlXuVxI
210. XXE demo - https://www.youtube.com/watch?v=3B8QhyrEXlU
211. XXE demo 2 - https://www.youtube.com/watch?v=UQjxvEwyUUw
212. XXE demo 3 - https://www.youtube.com/watch?v=JI0daBHq6fA

LDAP injection

213. Introduction and practical 1 - https://www.youtube.com/watch?v=-TXFlg7S9ks
214. Practical 2 - https://www.youtube.com/watch?v=wtahzm_R8e4

OS command injection

215. OS command injection in bWAPP - https://www.youtube.com/watch?v=qLIkGJrMY9k
216. bWAAP- OS command injection with Commiux (All levels) - https://www.youtube.com/watch?v=5-1QLbVa8YE

Local file inclusion

217. Detailed introduction - https://www.youtube.com/watch?v=kcojXEwolIs
218. LFI demo 1 - https://www.youtube.com/watch?v=54hSHpVoz7A

219. LFI demo 2 - https://www.youtube.com/watch?v=qPq9hIVtitI

Remote file inclusion

220. Detailed introduction - https://www.youtube.com/watch?v=MZjORTEwpaw
221. RFI demo 1 - https://www.youtube.com/watch?v=gWt9A6eOkq0
222. RFI introduction and demo 2 - https://www.youtube.com/watch?v=htTEfokaKsM

HTTP splitting/smuggling

223. Detailed introduction - https://www.youtube.com/watch?v=bVaZWHrfiPw
224. Demo 1 - https://www.youtube.com/watch?v=mOf4H1aLiiE

Phase 11 – Generating and testing error codes

225. Generating normal error codes by visiting files that may not exist on the server - for example visit chintan.php or chintan.aspx file on any website and it may redirect you to 404.php or 404.aspx or their customer error page. Check if an error page is generated by default web server or application framework or a custom page is displayed which does not display any sensitive information.
226. Use BurpSuite fuzzing techniques to generate stack trace error codes - https://www.youtube.com/watch?v=LDF6OkcvBzM

Phase 12 – Weak cryptography testing

227. SSL/TLS weak configuration explained - https://www.youtube.com/watch?v=Rp3iZUvXWlM
228. Testing weak SSL/TLS ciphers - https://www.youtube.com/watch?v=slbwCMHqCkc
229. Test SSL/TLS security with Qualys guard - https://www.youtube.com/watch?v=Na8KxqmETnw
230. Sensitive information sent via unencrypted channels - https://www.youtube.com/watch?v=21_IYz4npRs

Phase 12 – Business logic vulnerability

231. What is a business logic flaw - https://www.youtube.com/watch?v=ICbvQzva6lE&list=PLWoDr1kTbIxKZe_JeTDIcD2I7Uy1pLIFI
232. The Difficulties Finding Business Logic Vulnerabilities with Traditional Security Tools - https://www.youtube.com/watch?v=JTMg0bhkUbo&list=PLWoDr1kTbIxKZe_JeTDIcD2I7Uy1pLIFI&index=2
233. How To Identify Business Logic Flaws - https://www.youtube.com/watch?v=FJcgfLM4SAY&list=PLWoDr1kTbIxKZe_JeTDIcD2I7Uy1pLIFI&index=3
234. Business Logic Flaws: Attacker Mindset - https://www.youtube.com/watch?v=Svxh9KSTL3Y&list=PLWoDr1kTbIxKZe_JeTDIcD2I7Uy1pLIFI&index=4
235. Business Logic Flaws: Dos Attack On Resource - https://www.youtube.com/watch?v=4S6HWzhmXQk&list=PLWoDr1kTbIxKZe_JeTDIcD2I7Uy1pLIFI&index=5
236. Business Logic Flaws: Abuse Cases: Information Disclosure - https://www.youtube.com/watch?v=HrHdUEUwMHk&list=PLWoDr1kTbIxKZe_JeTDIcD2I7Uy1pLIFI&index=6

237. Business Logic Flaws: Abuse Cases: iPod Repairman Dupes Apple - https://www.youtube.com/watch?v=8yB_ApVsdhA&list=PLWoDr1kTbIxKZe_JeTDIcD2I7Uy1pLIFI&index=7
238. Business Logic Flaws: Abuse Cases: Online Auction - https://www.youtube.com/watch?v=oa_UICCqfbY&list=PLWoDr1kTbIxKZe_JeTDIcD2I7Uy1pLIFI&index=8
239. Business Logic Flaws: How To Navigate Code Using ShiftLeft Ocular - https://www.youtube.com/watch?v=hz7IZu6H6oE&list=PLWoDr1kTbIxKZe_JeTDIcD2I7Uy1pLIFI&index=9
240. Business Logic Security Checks: Data Privacy Compliance - https://www.youtube.com/watch?v=qX2fyniKUIQ&list=PLWoDr1kTbIxKZe_JeTDIcD2I7Uy1pLIFI&index=10
241. Business Logic Security Checks: Encryption Compliance - https://www.youtube.com/watch?v=V8zphJbltDY&list=PLWoDr1kTbIxKZe_JeTDIcD2I7Uy1pLIFI&index=11
242. Business Logic Security: Enforcement Checks - https://www.youtube.com/watch?v=5e7qgY_L3UQ&list=PLWoDr1kTbIxKZe_JeTDIcD2I7Uy1pLIFI&index=12
243. Business Logic Exploits: SQL Injection - https://www.youtube.com/watch?v=hcIysfhA9AA&list=PLWoDr1kTbIxKZe_JeTDIcD2I7Uy1pLIFI&index=13
244. Business Logic Exploits: Security Misconfiguration - https://www.youtube.com/watch?v=ppLBtCQcYRk&list=PLWoDr1kTbIxKZe_JeTDIcD2I7Uy1pLIFI&index=15
245. Business Logic Exploits: Data Leakage - https://www.youtube.com/watch?v=qe0bEvguvbs&list=PLWoDr1kTbIxKZe_JeTDIcD2I7Uy1pLIFI&index=16
246. Demo 1 - https://www.youtube.com/watch?v=yV7O-QRyOao
247. Demo 2 - https://www.youtube.com/watch?v=mzjTG7pKmQI
248. Demo 3 - https://www.youtube.com/watch?v=A8V_58QZPMs
249. Demo 4 - https://www.youtube.com/watch?v=1pvrEKAFJyk
250. Demo 5 - https://hackerone.com/reports/145745
251. Demo 6 - https://hackerone.com/reports/430854