**Web Application Penetration Testing**

**Phase 1 – History**

1. History of Internet - [https://www.youtube.com/watch?v=9hIQjrMHTv4](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D9hIQjrMHTv4%26amp;sa%3DD%26amp;ust%3D1534302195629000&sa=D&ust=1534302195761000&usg=AFQjCNHS93ZRCyiBT2kUR1krg3zouM6lHA)

**Phase 2 – Web and Server Technology**

1. Basic concepts of web applications, how they work and the HTTP protocol - [https://www.youtube.com/watch?v=RsQ1tFLwldY&t=7s](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DRsQ1tFLwldY%2526t%253D7s%26amp;sa%3DD%26amp;ust%3D1534302195630000&sa=D&ust=1534302195762000&usg=AFQjCNEH6VK4EP-L4W5Qo4rAoksTlqVzOA)
2. HTML basics part 1 - [https://www.youtube.com/watch?v=p6fRBGI\_BY0](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253Dp6fRBGI_BY0%26amp;sa%3DD%26amp;ust%3D1534302195631000&sa=D&ust=1534302195762000&usg=AFQjCNENRaLSHJEhvNJpGHNM3PphmJYyeQ)
3. HTML basics part 2 - [https://www.youtube.com/watch?v=Zs6lzuBVK2w](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DZs6lzuBVK2w%26amp;sa%3DD%26amp;ust%3D1534302195632000&sa=D&ust=1534302195762000&usg=AFQjCNEjzzlnJFm_uQRFbmfi6_cvM2Y_kg)
4. Difference between static and dynamic website - [https://www.youtube.com/watch?v=hlg6q6OFoxQ](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253Dhlg6q6OFoxQ%26amp;sa%3DD%26amp;ust%3D1534302195632000&sa=D&ust=1534302195762000&usg=AFQjCNE1dcZSPHm5yhzM3QZ-eAyGjmhOlQ)
5. HTTP protocol Understanding - [https://www.youtube.com/watch?v=JFZMyhRTVt0](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DJFZMyhRTVt0%26amp;sa%3DD%26amp;ust%3D1534302195632000&sa=D&ust=1534302195762000&usg=AFQjCNEXlDdlfhh1F-dCX7y8HrZlJ_DfPQ)
6. Parts of HTTP Request -[https://www.youtube.com/watch?v=pHFWGN-upGM](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DpHFWGN-upGM%26amp;sa%3DD%26amp;ust%3D1534302195633000&sa=D&ust=1534302195762000&usg=AFQjCNFEIPbnU96QlS-_nVd48QG1mjQYrw)
7. Parts of HTTP Response - [https://www.youtube.com/watch?v=c9sMNc2PrMU](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253Dc9sMNc2PrMU%26amp;sa%3DD%26amp;ust%3D1534302195633000&sa=D&ust=1534302195763000&usg=AFQjCNEXREz2QCE32iAoCPJ5BOddITYqFA)
8. Various HTTP Methods - [https://www.youtube.com/watch?v=PO7D20HsFsY](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DPO7D20HsFsY%26amp;sa%3DD%26amp;ust%3D1534302195634000&sa=D&ust=1534302195763000&usg=AFQjCNETdhDWoD4864GuWYq9wg3UHhqRzA)
9. Understanding URLS - [https://www.youtube.com/watch?v=5Jr-\_Za5yQM](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D5Jr-_Za5yQM%26amp;sa%3DD%26amp;ust%3D1534302195634000&sa=D&ust=1534302195763000&usg=AFQjCNEv0B3c4mI8hVw9PJMF2_wwLo5lhQ)
10. Intro to REST - [https://www.youtube.com/watch?v=YCcAE2SCQ6k](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DYCcAE2SCQ6k%26amp;sa%3DD%26amp;ust%3D1534302195635000&sa=D&ust=1534302195763000&usg=AFQjCNFh24_U-ECaPncMHUkAVlJQcj02IQ)
11. HTTP Request & Response Headers - [https://www.youtube.com/watch?v=vAuZwirKjWs](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DvAuZwirKjWs%26amp;sa%3DD%26amp;ust%3D1534302195635000&sa=D&ust=1534302195763000&usg=AFQjCNF740J4frxRpHR76HCcJWIxbOTCGQ)
12. What is a cookie - [https://www.youtube.com/watch?v=I01XMRo2ESg](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DI01XMRo2ESg%26amp;sa%3DD%26amp;ust%3D1534302195636000&sa=D&ust=1534302195764000&usg=AFQjCNFd4G-9PxkdEAf2DpsB9dtZCQ9hcw)
13. HTTP Status codes - [https://www.youtube.com/watch?v=VLH3FMQ5BIQ](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DVLH3FMQ5BIQ%26amp;sa%3DD%26amp;ust%3D1534302195636000&sa=D&ust=1534302195764000&usg=AFQjCNEwPijLYb4QBQMdBRMfwvVnZgEKFg)
14. HTTP Proxy - [https://www.youtube.com/watch?v=qU0PVSJCKcs](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DqU0PVSJCKcs%26amp;sa%3DD%26amp;ust%3D1534302195637000&sa=D&ust=1534302195764000&usg=AFQjCNGTkqqzPSCTR24xaZfXar9Ge5oWMg)
15. Authentication with HTTP - [https://www.youtube.com/watch?v=GxiFXUFKo1M](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DGxiFXUFKo1M%26amp;sa%3DD%26amp;ust%3D1534302195637000&sa=D&ust=1534302195764000&usg=AFQjCNEwJGSH4Thqvxshd_9iTWLmYgVUMA)
16. HTTP basic and digest authentication - [https://www.youtube.com/watch?v=GOnhCbDhMzk](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DGOnhCbDhMzk%26amp;sa%3DD%26amp;ust%3D1534302195637000&sa=D&ust=1534302195764000&usg=AFQjCNEdTPZludYiPHVQBAyMaVE4kEjauQ)
17. What is “Server-Side” - [https://www.youtube.com/watch?v=JnCLmLO9LhA](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DJnCLmLO9LhA%26amp;sa%3DD%26amp;ust%3D1534302195638000&sa=D&ust=1534302195764000&usg=AFQjCNE0ubX5pU6mFGGfyYM7EnzhH1Wueg)
18. Server and client side with example - [https://www.youtube.com/watch?v=DcBB2Fp8WNI](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DDcBB2Fp8WNI%26amp;sa%3DD%26amp;ust%3D1534302195638000&sa=D&ust=1534302195765000&usg=AFQjCNEDODYQVTZb-ZF2HDBkIGnNkzj7Hw)
19. What is a session - [https://www.youtube.com/watch?v=WV4DJ6b0jhg&t=202s](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DWV4DJ6b0jhg%2526t%253D202s%26amp;sa%3DD%26amp;ust%3D1534302195639000&sa=D&ust=1534302195765000&usg=AFQjCNGo8vaAqF10vy2UurwEZhdW20_bhg)
20. Introduction to UTF-8 and Unicode - [https://www.youtube.com/watch?v=sqPTR\_v4qFA](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DsqPTR_v4qFA%26amp;sa%3DD%26amp;ust%3D1534302195639000&sa=D&ust=1534302195765000&usg=AFQjCNEr8Ty7Sdxq4j_EelV8pjnJctdfpg)
21. URL encoding - [https://www.youtube.com/watch?v=Z3udiqgW1VA](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DZ3udiqgW1VA%26amp;sa%3DD%26amp;ust%3D1534302195639000&sa=D&ust=1534302195765000&usg=AFQjCNH9qi0we5mKK5jMLqC8Mv6T0JOceA)
22. HTML encoding - [https://www.youtube.com/watch?v=IiAfCLWpgII&t=109s](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DIiAfCLWpgII%2526t%253D109s%26amp;sa%3DD%26amp;ust%3D1534302195640000&sa=D&ust=1534302195765000&usg=AFQjCNF2gM2QmgS8OQl7qBX1IA_r-ekflQ)
23. Base64 encoding - [https://www.youtube.com/watch?v=8qkxeZmKmOY](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D8qkxeZmKmOY%26amp;sa%3DD%26amp;ust%3D1534302195640000&sa=D&ust=1534302195766000&usg=AFQjCNH3UP07EcAvPvAbH_LUdbA-Ey1-AQ)
24. Hex encoding & ASCII - [https://www.youtube.com/watch?v=WW2SaCMnHdU](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DWW2SaCMnHdU%26amp;sa%3DD%26amp;ust%3D1534302195640000&sa=D&ust=1534302195766000&usg=AFQjCNGKUPZrQjiUn7EIG0qT-dm02XchIA)

**Phase 3 – Setting up the lab with BurpSuite and bWAPP**

**MANISH AGRAWAL**

1. Setup lab with bWAPP - https://www.youtube.com/watch?v=dwtUn3giwTk&index=1&list=PLv95pq8fEyuivHeZB2jeC435tU3\_1YGzV
2. Set up Burp Suite -  [https://www.youtube.com/watch?v=hQsT4rSa\_v0&list=PLv95pq8fEyuivHeZB2jeC435tU3\_1YGzV&index=2](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DhQsT4rSa_v0%2526list%253DPLv95pq8fEyuivHeZB2jeC435tU3_1YGzV%2526index%253D2%26amp;sa%3DD%26amp;ust%3D1534302195642000&sa=D&ust=1534302195766000&usg=AFQjCNFTNSFhzml-AKGZbFQPuP2FDHqfig)
3. Configure Firefox and add certificate - [https://www.youtube.com/watch?v=hfsdJ69GSV4&index=3&list=PLv95pq8fEyuivHeZB2jeC435tU3\_1YGzV](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DhfsdJ69GSV4%2526index%253D3%2526list%253DPLv95pq8fEyuivHeZB2jeC435tU3_1YGzV%26amp;sa%3DD%26amp;ust%3D1534302195642000&sa=D&ust=1534302195767000&usg=AFQjCNHcf9YEIaM9ycjFuK-ZgOlR5OkpBQ)
4. Mapping and scoping website - [https://www.youtube.com/watch?v=H-\_iVteMDRo&index=4&list=PLv95pq8fEyuivHeZB2jeC435tU3\_1YGzV](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DH-_iVteMDRo%2526index%253D4%2526list%253DPLv95pq8fEyuivHeZB2jeC435tU3_1YGzV%26amp;sa%3DD%26amp;ust%3D1534302195643000&sa=D&ust=1534302195767000&usg=AFQjCNGIEpX5rCrAiDXWkAQ1blyFVJVS0w)
5. Spidering - [https://www.youtube.com/watch?v=97uMUQGIe14&list=PLv95pq8fEyuivHeZB2jeC435tU3\_1YGzV&index=5](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D97uMUQGIe14%2526list%253DPLv95pq8fEyuivHeZB2jeC435tU3_1YGzV%2526index%253D5%26amp;sa%3DD%26amp;ust%3D1534302195643000&sa=D&ust=1534302195767000&usg=AFQjCNHMMXNlAmgh9vNHmpOL3UpR6y9OWA)
6. Active and passive scanning - [https://www.youtube.com/watch?v=1Mjom6AcFyU&index=6&list=PLv95pq8fEyuivHeZB2jeC435tU3\_1YGzV](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D1Mjom6AcFyU%2526index%253D6%2526list%253DPLv95pq8fEyuivHeZB2jeC435tU3_1YGzV%26amp;sa%3DD%26amp;ust%3D1534302195645000&sa=D&ust=1534302195767000&usg=AFQjCNFOUdrn3MWDoTmtZs48CiGxPB0Q3A)
7. Scanner options and demo - [https://www.youtube.com/watch?v=gANi4Kt7-ek&index=7&list=PLv95pq8fEyuivHeZB2jeC435tU3\_1YGzV](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DgANi4Kt7-ek%2526index%253D7%2526list%253DPLv95pq8fEyuivHeZB2jeC435tU3_1YGzV%26amp;sa%3DD%26amp;ust%3D1534302195645000&sa=D&ust=1534302195767000&usg=AFQjCNE59V7bvjbSA4muLLjtFYANP3I3ag)
8. Introduction to password security - [https://www.youtube.com/watch?v=FwcUhcLO9iM&list=PLv95pq8fEyuivHeZB2jeC435tU3\_1YGzV&index=8](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DFwcUhcLO9iM%2526list%253DPLv95pq8fEyuivHeZB2jeC435tU3_1YGzV%2526index%253D8%26amp;sa%3DD%26amp;ust%3D1534302195646000&sa=D&ust=1534302195767000&usg=AFQjCNF1u7F1ct18JCzKNgHTqbsEFAYWeQ)
9. Intruder - [https://www.youtube.com/watch?v=wtMg9oEMTa8&list=PLv95pq8fEyuivHeZB2jeC435tU3\_1YGzV&index=9](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DwtMg9oEMTa8%2526list%253DPLv95pq8fEyuivHeZB2jeC435tU3_1YGzV%2526index%253D9%26amp;sa%3DD%26amp;ust%3D1534302195647000&sa=D&ust=1534302195768000&usg=AFQjCNFoeYO3VHat4yHXmxp7-8al44ecvg)
10. Intruder attack types - [https://www.youtube.com/watch?v=N5ndYPwddkQ&index=10&list=PLv95pq8fEyuivHeZB2jeC435tU3\_1YGzV](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DN5ndYPwddkQ%2526index%253D10%2526list%253DPLv95pq8fEyuivHeZB2jeC435tU3_1YGzV%26amp;sa%3DD%26amp;ust%3D1534302195647000&sa=D&ust=1534302195768000&usg=AFQjCNFo-KKSbRWMpQ5Igh8FciKh2m_Ylw)
11. Payload settings - [https://www.youtube.com/watch?v=5GpdlbtL-1Q&index=11&list=PLv95pq8fEyuivHeZB2jeC435tU3\_1YGzV](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D5GpdlbtL-1Q%2526index%253D11%2526list%253DPLv95pq8fEyuivHeZB2jeC435tU3_1YGzV%26amp;sa%3DD%26amp;ust%3D1534302195648000&sa=D&ust=1534302195768000&usg=AFQjCNGIsTYl1anPMq1RCLdXeq-PRrnvfQ)
12. Intruder settings - [https://www.youtube.com/watch?v=B\_Mu7jmOYnU&list=PLv95pq8fEyuivHeZB2jeC435tU3\_1YGzV&index=12](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DB_Mu7jmOYnU%2526list%253DPLv95pq8fEyuivHeZB2jeC435tU3_1YGzV%2526index%253D12%26amp;sa%3DD%26amp;ust%3D1534302195648000&sa=D&ust=1534302195768000&usg=AFQjCNH7S4n30Jf-BXkWQxi0LVLS47DlzQ)

[**ÆTHER SECURITY LAB**](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/channel/UCq_h2sGrbWA2JzJ1HjDMXcQ%26amp;sa%3DD%26amp;ust%3D1534302195648000&sa=D&ust=1534302195768000&usg=AFQjCNERw60EGFbG_KFq_dso5Ejw9fOuYg)

1. No.1 Penetration testing tool - [https://www.youtube.com/watch?v=AVzC7ETqpDo&list=PLq9n8iqQJFDrwFe9AEDBlR1uSHEN7egQA&index=1](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DAVzC7ETqpDo%2526list%253DPLq9n8iqQJFDrwFe9AEDBlR1uSHEN7egQA%2526index%253D1%26amp;sa%3DD%26amp;ust%3D1534302195649000&sa=D&ust=1534302195769000&usg=AFQjCNF0lR0_4IVy4XpyCjg-0AUmlIdXoQ)
2. Environment Setup - [https://www.youtube.com/watch?v=yqnUOdr0eVk&index=2&list=PLq9n8iqQJFDrwFe9AEDBlR1uSHEN7egQA](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DyqnUOdr0eVk%2526index%253D2%2526list%253DPLq9n8iqQJFDrwFe9AEDBlR1uSHEN7egQA%26amp;sa%3DD%26amp;ust%3D1534302195649000&sa=D&ust=1534302195769000&usg=AFQjCNGaNWvnFlIQnEl_M5tKRdNjSPHQOA)
3. General concept - [https://www.youtube.com/watch?v=udl4oqr\_ylM&list=PLq9n8iqQJFDrwFe9AEDBlR1uSHEN7egQA&index=3](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253Dudl4oqr_ylM%2526list%253DPLq9n8iqQJFDrwFe9AEDBlR1uSHEN7egQA%2526index%253D3%26amp;sa%3DD%26amp;ust%3D1534302195650000&sa=D&ust=1534302195769000&usg=AFQjCNHbNl6NyC_yCi7Kg6LGQWd_QUUSCA)
4. Proxy module - [https://www.youtube.com/watch?v=PDTwYFkjQBE&list=PLq9n8iqQJFDrwFe9AEDBlR1uSHEN7egQA&index=4](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DPDTwYFkjQBE%2526list%253DPLq9n8iqQJFDrwFe9AEDBlR1uSHEN7egQA%2526index%253D4%26amp;sa%3DD%26amp;ust%3D1534302195650000&sa=D&ust=1534302195769000&usg=AFQjCNFk458VCRHlGf9WVkft3KjSY1yQPA)
5. Repeater module - [https://www.youtube.com/watch?v=9Zh\_7s5csCc&list=PLq9n8iqQJFDrwFe9AEDBlR1uSHEN7egQA&index=5](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D9Zh_7s5csCc%2526list%253DPLq9n8iqQJFDrwFe9AEDBlR1uSHEN7egQA%2526index%253D5%26amp;sa%3DD%26amp;ust%3D1534302195651000&sa=D&ust=1534302195769000&usg=AFQjCNGpYR7CtJVNDCbUjeJwkakyGZsk_g)
6. Target and spider module - [https://www.youtube.com/watch?v=dCKPZUSOlr8&list=PLq9n8iqQJFDrwFe9AEDBlR1uSHEN7egQA&index=6](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DdCKPZUSOlr8%2526list%253DPLq9n8iqQJFDrwFe9AEDBlR1uSHEN7egQA%2526index%253D6%26amp;sa%3DD%26amp;ust%3D1534302195651000&sa=D&ust=1534302195770000&usg=AFQjCNGAlcOD4VVWP8uoNY-n1efeO4zcdw)
7. Sequencer and scanner module - [https://www.youtube.com/watch?v=G-v581pXerE&list=PLq9n8iqQJFDrwFe9AEDBlR1uSHEN7egQA&index=7](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DG-v581pXerE%2526list%253DPLq9n8iqQJFDrwFe9AEDBlR1uSHEN7egQA%2526index%253D7%26amp;sa%3DD%26amp;ust%3D1534302195652000&sa=D&ust=1534302195770000&usg=AFQjCNF-ti9hizTCiGSGG5cbOGvucxzHSQ)

**Phase 4 – Mapping the application and attack surface**

1. Spidering - [https://www.youtube.com/watch?v=97uMUQGIe14&list=PLv95pq8fEyuivHeZB2jeC435tU3\_1YGzV&index=5](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D97uMUQGIe14%2526list%253DPLv95pq8fEyuivHeZB2jeC435tU3_1YGzV%2526index%253D5%26amp;sa%3DD%26amp;ust%3D1534302195652000&sa=D&ust=1534302195770000&usg=AFQjCNH7GNQy6Bh6TpIA7-u2rni1OtjsMQ)
2. Mapping application using robots.txt - [https://www.youtube.com/watch?v=akuzgZ75zrk](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DakuzgZ75zrk%26amp;sa%3DD%26amp;ust%3D1534302195652000&sa=D&ust=1534302195770000&usg=AFQjCNG4KQ3oxNCphkkMmzj_oaAL97dGyw)
3. Discover hidden contents using dirbuster - [https://www.youtube.com/watch?v=--nu9Jq07gA](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D--nu9Jq07gA%26amp;sa%3DD%26amp;ust%3D1534302195653000&sa=D&ust=1534302195770000&usg=AFQjCNFI8oMmxqhUNvs-dkrznyLbEZC6vA)
4. Dirbuster in detail - [https://www.youtube.com/watch?v=2tOQC68hAcQ](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D2tOQC68hAcQ%26amp;sa%3DD%26amp;ust%3D1534302195653000&sa=D&ust=1534302195770000&usg=AFQjCNHkUcIYcMpqP5kU0OOXBmT5BFMSFQ)
5. Discover hidden directories and files with intruder - [https://www.youtube.com/watch?v=4Fz9mJeMNkI](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D4Fz9mJeMNkI%26amp;sa%3DD%26amp;ust%3D1534302195653000&sa=D&ust=1534302195771000&usg=AFQjCNGpH6QMaDUaOFjgWVYAZrJTCGMB-Q)
6. Identify application entry points - [https://www.youtube.com/watch?v=IgJWPZ2OKO8&t=34s](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DIgJWPZ2OKO8%2526t%253D34s%26amp;sa%3DD%26amp;ust%3D1534302195654000&sa=D&ust=1534302195771000&usg=AFQjCNFoWG8P1Ex0XRHf1z-bjHHnTslWzQ)
7. Identify application entry points - [https://www.owasp.org/index.php/Identify\_application\_entry\_points\_(OTG-INFO-006)](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.owasp.org/index.php/Identify_application_entry_points_(OTG-INFO-006)%26amp;sa%3DD%26amp;ust%3D1534302195654000&sa=D&ust=1534302195771000&usg=AFQjCNElSAks9KOPukFi5kdyubni6RlHow)
8. Identify client and server technology - [https://www.youtube.com/watch?v=B8jN\_iWjtyM](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DB8jN_iWjtyM%26amp;sa%3DD%26amp;ust%3D1534302195655000&sa=D&ust=1534302195771000&usg=AFQjCNEwoFMkmQmgM-Y5nP-nHTcPhqM0pw)
9. Identify server technology using banner grabbing (telnet) - [https://www.youtube.com/watch?v=O67M-U2UOAg](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DO67M-U2UOAg%26amp;sa%3DD%26amp;ust%3D1534302195655000&sa=D&ust=1534302195771000&usg=AFQjCNH6y0L3SR8e9LqEVGeQe2OLexmuTA)
10. Identify server technology using httprecon - [https://www.youtube.com/watch?v=xBBHtS-dwsM](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DxBBHtS-dwsM%26amp;sa%3DD%26amp;ust%3D1534302195655000&sa=D&ust=1534302195771000&usg=AFQjCNGHzz0l9J-v0c-RSi4s_kqy7f883w)

**Phase 5 – Understanding and exploiting OWASP top 10 vulnerabilities**

1. A closer look at all owasp top 10 vulnerabilities - [https://www.youtube.com/watch?v=avFR\_Af0KGk](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DavFR_Af0KGk%26amp;sa%3DD%26amp;ust%3D1534302195656000&sa=D&ust=1534302195772000&usg=AFQjCNHufcdrvhmDdUGEvh11Bi1huJlNGw)

**IBM**

1. Injection  - [https://www.youtube.com/watch?v=02mLrFVzIYU&index=1&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D02mLrFVzIYU%2526index%253D1%2526list%253DPLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d%26amp;sa%3DD%26amp;ust%3D1534302195657000&sa=D&ust=1534302195772000&usg=AFQjCNF7XEZo1gqCbuTXdWsSc2ypP0boCg)
2. Broken authentication and session management - [https://www.youtube.com/watch?v=iX49fqZ8HGA&index=2&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DiX49fqZ8HGA%2526index%253D2%2526list%253DPLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d%26amp;sa%3DD%26amp;ust%3D1534302195658000&sa=D&ust=1534302195772000&usg=AFQjCNE5gXLcqPLmNLL9oLUnLmITgql5-g)
3. Cross-site scripting  - [https://www.youtube.com/watch?v=x6I5fCupLLU&index=3&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253Dx6I5fCupLLU%2526index%253D3%2526list%253DPLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d%26amp;sa%3DD%26amp;ust%3D1534302195658000&sa=D&ust=1534302195772000&usg=AFQjCNFgebsX7NR_47zNJqXldWHzRcDwVQ)
4. Insecure direct object reference  - [https://www.youtube.com/watch?v=-iCyp9Qz3CI&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d&index=4](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D-iCyp9Qz3CI%2526list%253DPLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d%2526index%253D4%26amp;sa%3DD%26amp;ust%3D1534302195659000&sa=D&ust=1534302195772000&usg=AFQjCNHztd_6sFFxVrC7jrLfnaxd7ldS6w)
5. Security misconfiguration  - [https://www.youtube.com/watch?v=cIplXL8idyo&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d&index=5](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DcIplXL8idyo%2526list%253DPLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d%2526index%253D5%26amp;sa%3DD%26amp;ust%3D1534302195659000&sa=D&ust=1534302195773000&usg=AFQjCNERIR7vXADt6yWjt3Dz9GXviyjIXQ)
6. Sensitive data exposure  - [https://www.youtube.com/watch?v=rYlzTQlF8Ws&index=6&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DrYlzTQlF8Ws%2526index%253D6%2526list%253DPLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d%26amp;sa%3DD%26amp;ust%3D1534302195659000&sa=D&ust=1534302195773000&usg=AFQjCNEGtBafG1_hx1QZ0aJrffP9Wr9wVw)
7. Missing functional level access controls  - [https://www.youtube.com/watch?v=VMv\_gyCNGpk&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d&index=7](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DVMv_gyCNGpk%2526list%253DPLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d%2526index%253D7%26amp;sa%3DD%26amp;ust%3D1534302195660000&sa=D&ust=1534302195773000&usg=AFQjCNFiq4S-pG4drl8fd88wqQc1CC8Ung)
8. Cross-site request forgery  - [https://www.youtube.com/watch?v=\_xSFm3KGxh0&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d&index=8](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D_xSFm3KGxh0%2526list%253DPLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d%2526index%253D8%26amp;sa%3DD%26amp;ust%3D1534302195660000&sa=D&ust=1534302195773000&usg=AFQjCNEbJQmEPq8XF0f-KuaHkHm8fyRyYw)
9. Using components with known vulnerabilities   - [https://www.youtube.com/watch?v=bhJmVBJ-F-4&index=9&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DbhJmVBJ-F-4%2526index%253D9%2526list%253DPLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d%26amp;sa%3DD%26amp;ust%3D1534302195660000&sa=D&ust=1534302195773000&usg=AFQjCNGgDx8oaP_V2CPMVu0S-npRzU8-Dg)
10. Unvalidated redirects and forwards  - [https://www.youtube.com/watch?v=L6bYKiLtSL8&index=10&list=PLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DL6bYKiLtSL8%2526index%253D10%2526list%253DPLoyY7ZjHtUUVLs2fy-ctzZDSPpawuQ28d%26amp;sa%3DD%26amp;ust%3D1534302195661000&sa=D&ust=1534302195773000&usg=AFQjCNHEctfhwT8HJGDUaUGQ03FNEqhm8Q)

**F5 CENTRAL**

1. Injection - [https://www.youtube.com/watch?v=rWHvp7rUka8&index=1&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H\_jD](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DrWHvp7rUka8%2526index%253D1%2526list%253DPLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD%26amp;sa%3DD%26amp;ust%3D1534302195662000&sa=D&ust=1534302195774000&usg=AFQjCNFAbB_Pi0unBqlk1_tg4TRxep3rbg)
2. Broken authentication and session management  - [https://www.youtube.com/watch?v=mruO75ONWy8&index=2&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H\_jD](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DmruO75ONWy8%2526index%253D2%2526list%253DPLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD%26amp;sa%3DD%26amp;ust%3D1534302195662000&sa=D&ust=1534302195774000&usg=AFQjCNEqllY1E9uiUJbwX8DdamwmuWL_hA)
3. Insecure deserialisation  - [https://www.youtube.com/watch?v=nkTBwbnfesQ&index=8&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H\_jD](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DnkTBwbnfesQ%2526index%253D8%2526list%253DPLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD%26amp;sa%3DD%26amp;ust%3D1534302195663000&sa=D&ust=1534302195774000&usg=AFQjCNFL05pcW3MkxLkGorP-IP4DXk-raw)
4. Sensitive data exposure  - [https://www.youtube.com/watch?v=2RKbacrkUBU&index=3&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H\_jD](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D2RKbacrkUBU%2526index%253D3%2526list%253DPLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD%26amp;sa%3DD%26amp;ust%3D1534302195663000&sa=D&ust=1534302195774000&usg=AFQjCNHqX9IoMXIVckXnPRH-q-KpBOsrIw)
5. Broken access control  - [https://www.youtube.com/watch?v=P38at6Tp8Ms&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H\_jD&index=5](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DP38at6Tp8Ms%2526list%253DPLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD%2526index%253D5%26amp;sa%3DD%26amp;ust%3D1534302195663000&sa=D&ust=1534302195774000&usg=AFQjCNG_TRM7b5i-Rib1yzp9ZIk6gFkXEQ)
6. Insufficient logging and monitoring  - [https://www.youtube.com/watch?v=IFF3tkUOF5E&index=10&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H\_jD](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DIFF3tkUOF5E%2526index%253D10%2526list%253DPLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD%26amp;sa%3DD%26amp;ust%3D1534302195664000&sa=D&ust=1534302195775000&usg=AFQjCNFMhJfY8T2uLSFn_z6vMjlxbn0Dng)
7. XML external entities  - [https://www.youtube.com/watch?v=g2ey7ry8\_CQ&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H\_jD&index=4](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253Dg2ey7ry8_CQ%2526list%253DPLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD%2526index%253D4%26amp;sa%3DD%26amp;ust%3D1534302195665000&sa=D&ust=1534302195775000&usg=AFQjCNH-4qzoNHrAdD1do8OQ-N2Ykm7NLQ)
8. Using components with known vulnerabilities  - [https://www.youtube.com/watch?v=IGsNYVDKRV0&index=9&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H\_jD](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DIGsNYVDKRV0%2526index%253D9%2526list%253DPLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD%26amp;sa%3DD%26amp;ust%3D1534302195666000&sa=D&ust=1534302195775000&usg=AFQjCNHxolX6GMXclw3Wvler73an5waIVg)
9. Cross-site scripting  - [https://www.youtube.com/watch?v=IuzU4y-UjLw&index=7&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H\_jD](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DIuzU4y-UjLw%2526index%253D7%2526list%253DPLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD%26amp;sa%3DD%26amp;ust%3D1534302195666000&sa=D&ust=1534302195775000&usg=AFQjCNHZtXBhdUfVA3YgAdx0T3Yt_Drqkw)
10. Security misconfiguration  - [https://www.youtube.com/watch?v=JuGSUMtKTPU&index=6&list=PLyqga7AXMtPPuibxp1N0TdyDrKwP9H\_jD](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DJuGSUMtKTPU%2526index%253D6%2526list%253DPLyqga7AXMtPPuibxp1N0TdyDrKwP9H_jD%26amp;sa%3DD%26amp;ust%3D1534302195666000&sa=D&ust=1534302195775000&usg=AFQjCNEHpagnF4TcHwVQDvC4ABkVWb39FQ)

**LUKE BRINER**

1. Injection explained - [https://www.youtube.com/watch?v=1qMggPJpRXM&index=1&list=PLpNYlUeSK\_rkrrBox-xvSkm5lgaDqKa0X](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D1qMggPJpRXM%2526index%253D1%2526list%253DPLpNYlUeSK_rkrrBox-xvSkm5lgaDqKa0X%26amp;sa%3DD%26amp;ust%3D1534302195668000&sa=D&ust=1534302195776000&usg=AFQjCNE6b3Pl4ABMKzPPUlCMVQVrqhsmwA)
2. Broken authentication and session management - [https://www.youtube.com/watch?v=fKnG15BL4AY&list=PLpNYlUeSK\_rkrrBox-xvSkm5lgaDqKa0X&index=2](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DfKnG15BL4AY%2526list%253DPLpNYlUeSK_rkrrBox-xvSkm5lgaDqKa0X%2526index%253D2%26amp;sa%3DD%26amp;ust%3D1534302195668000&sa=D&ust=1534302195776000&usg=AFQjCNH5wOqljS0Q_fXziwOz1ICeSv83WA)
3. Cross-site scripting - [https://www.youtube.com/watch?v=ksM-xXeDUNs&index=3&list=PLpNYlUeSK\_rkrrBox-xvSkm5lgaDqKa0X](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DksM-xXeDUNs%2526index%253D3%2526list%253DPLpNYlUeSK_rkrrBox-xvSkm5lgaDqKa0X%26amp;sa%3DD%26amp;ust%3D1534302195669000&sa=D&ust=1534302195776000&usg=AFQjCNESmFGD_cvi67-uk5ygZKJasChU3w)
4. Insecure direct object reference - [https://www.youtube.com/watch?v=ZodA76-CB10&list=PLpNYlUeSK\_rkrrBox-xvSkm5lgaDqKa0X&index=4](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DZodA76-CB10%2526list%253DPLpNYlUeSK_rkrrBox-xvSkm5lgaDqKa0X%2526index%253D4%26amp;sa%3DD%26amp;ust%3D1534302195669000&sa=D&ust=1534302195776000&usg=AFQjCNGEEyUqqGXoJrKUtXKFtT0felwC7Q)
5. Security misconfiguration - [https://www.youtube.com/watch?v=DfFPHKPCofY&index=5&list=PLpNYlUeSK\_rkrrBox-xvSkm5lgaDqKa0X](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DDfFPHKPCofY%2526index%253D5%2526list%253DPLpNYlUeSK_rkrrBox-xvSkm5lgaDqKa0X%26amp;sa%3DD%26amp;ust%3D1534302195670000&sa=D&ust=1534302195776000&usg=AFQjCNEKZ9t_zPFqjErSbk-m7q6uKEO3FA)
6. Sensitive data exposure - [https://www.youtube.com/watch?v=Z7hafbGDVEE&list=PLpNYlUeSK\_rkrrBox-xvSkm5lgaDqKa0X&index=6](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DZ7hafbGDVEE%2526list%253DPLpNYlUeSK_rkrrBox-xvSkm5lgaDqKa0X%2526index%253D6%26amp;sa%3DD%26amp;ust%3D1534302195670000&sa=D&ust=1534302195776000&usg=AFQjCNFFmq4qdRtUMG8VDaAos45VWj6trw)
7. Missing functional level access control - [https://www.youtube.com/watch?v=RGN3w831Elo&list=PLpNYlUeSK\_rkrrBox-xvSkm5lgaDqKa0X&index=7](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DRGN3w831Elo%2526list%253DPLpNYlUeSK_rkrrBox-xvSkm5lgaDqKa0X%2526index%253D7%26amp;sa%3DD%26amp;ust%3D1534302195671000&sa=D&ust=1534302195777000&usg=AFQjCNFpe2TDQ6hmILLgicDDNFvrmRPZbg)
8. Cross-site request forgery - [https://www.youtube.com/watch?v=XRW\_US5BCxk&list=PLpNYlUeSK\_rkrrBox-xvSkm5lgaDqKa0X&index=8](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DXRW_US5BCxk%2526list%253DPLpNYlUeSK_rkrrBox-xvSkm5lgaDqKa0X%2526index%253D8%26amp;sa%3DD%26amp;ust%3D1534302195671000&sa=D&ust=1534302195777000&usg=AFQjCNGo0eGO-WxYywD3hao8oNwoX2snCg)
9. Components with known vulnerabilities - [https://www.youtube.com/watch?v=pbvDW9pJdng&list=PLpNYlUeSK\_rkrrBox-xvSkm5lgaDqKa0X&index=9](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DpbvDW9pJdng%2526list%253DPLpNYlUeSK_rkrrBox-xvSkm5lgaDqKa0X%2526index%253D9%26amp;sa%3DD%26amp;ust%3D1534302195672000&sa=D&ust=1534302195777000&usg=AFQjCNGAfVOEGQGX4I-GdxrOMk_bqT9nQw)
10. Unvalidated redirects and forwards - [https://www.youtube.com/watch?v=bHTglpgC5Qg&list=PLpNYlUeSK\_rkrrBox-xvSkm5lgaDqKa0X&index=10](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DbHTglpgC5Qg%2526list%253DPLpNYlUeSK_rkrrBox-xvSkm5lgaDqKa0X%2526index%253D10%26amp;sa%3DD%26amp;ust%3D1534302195672000&sa=D&ust=1534302195777000&usg=AFQjCNENexMaGyeOzEBtFUt5v10-9l9Jqg)

**Phase 6 – Bypassing client-side controls**

1. What is hidden forms in HTML - [https://www.youtube.com/watch?v=orUoGsgaYAE](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DorUoGsgaYAE%26amp;sa%3DD%26amp;ust%3D1534302195673000&sa=D&ust=1534302195777000&usg=AFQjCNFF-id0tdR2zo5ZolF3QviRB6ZrbQ)
2. Bypassing hidden form fields using tamper data - [https://www.youtube.com/watch?v=NXkGX2sPw7I](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DNXkGX2sPw7I%26amp;sa%3DD%26amp;ust%3D1534302195674000&sa=D&ust=1534302195777000&usg=AFQjCNFQNpdx51PqwMMMtNBvggkpARFF3w)
3. Bypassing hidden form fields using Burp Suite (Purchase application) - [https://www.youtube.com/watch?v=xahvJyUFTfM](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DxahvJyUFTfM%26amp;sa%3DD%26amp;ust%3D1534302195674000&sa=D&ust=1534302195778000&usg=AFQjCNE1p4-n4QfNh7Ww4Y-4Z8ruTE6NAg)
4. Changing price on eCommerce website using parameter tampering - [https://www.youtube.com/watch?v=A-ccNpP06Zg](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DA-ccNpP06Zg%26amp;sa%3DD%26amp;ust%3D1534302195675000&sa=D&ust=1534302195778000&usg=AFQjCNECwoZapqquy7_EuvHyek3TgFRnqg)
5. Understanding cookie in detail - [https://www.youtube.com/watch?v=\_P7KN8T1boc&list=PLWPirh4EWFpESKWJmrgQwmsnTrL\_K93Wi&index=18](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D_P7KN8T1boc%2526list%253DPLWPirh4EWFpESKWJmrgQwmsnTrL_K93Wi%2526index%253D18%26amp;sa%3DD%26amp;ust%3D1534302195675000&sa=D&ust=1534302195778000&usg=AFQjCNEY73vrZk8TCcoK-rhz6DXsW6QSgQ)
6. Cookie tampering with tamper data- [https://www.youtube.com/watch?v=NgKXm0lBecc](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DNgKXm0lBecc%26amp;sa%3DD%26amp;ust%3D1534302195675000&sa=D&ust=1534302195778000&usg=AFQjCNGbZ-vHB0Q0ewvZKqjk4rGgZM9p5Q)
7. Cookie tamper part 2 - [https://www.youtube.com/watch?v=dTCt\_I2DWgo](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DdTCt_I2DWgo%26amp;sa%3DD%26amp;ust%3D1534302195676000&sa=D&ust=1534302195778000&usg=AFQjCNFieEYjxrkyHzNfGtEbGfzSaDVpXw)
8. Understanding referer header in depth using Cisco product - [https://www.youtube.com/watch?v=GkQnBa3C7WI&t=35s](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DGkQnBa3C7WI%2526t%253D35s%26amp;sa%3DD%26amp;ust%3D1534302195676000&sa=D&ust=1534302195779000&usg=AFQjCNHsy7qn4UZR1_U3EwDiq9qeKAj2Pw)
9. Introduction to ASP.NET viewstate - [https://www.youtube.com/watch?v=L3p6Uw6SSXs](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DL3p6Uw6SSXs%26amp;sa%3DD%26amp;ust%3D1534302195676000&sa=D&ust=1534302195779000&usg=AFQjCNE3tD9YMCuZ8VKX0bUXKOWRhtRQAA)
10. ASP.NET viewstate in depth - [https://www.youtube.com/watch?v=Fn\_08JLsrmY](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DFn_08JLsrmY%26amp;sa%3DD%26amp;ust%3D1534302195677000&sa=D&ust=1534302195779000&usg=AFQjCNGlr0ZppqNkqNhTFzVYb0mBkKz4JQ)
11. Analyse sensitive data in ASP.NET viewstate - [https://msdn.microsoft.com/en-us/library/ms972427.aspx?f=255&MSPPError=-2147217396](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://msdn.microsoft.com/en-us/library/ms972427.aspx?f%253D255%2526MSPPError%253D-2147217396%26amp;sa%3DD%26amp;ust%3D1534302195677000&sa=D&ust=1534302195779000&usg=AFQjCNEnZM6zINXfRf0kEv5vIixSWWxcgA)

**Phase 7 – Attacking authentication/login**

1. Attacking login panel with bad password - Guess username password for the website and try different combinations
2. Brute-force login panel - [https://www.youtube.com/watch?v=25cazx5D\_vw](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D25cazx5D_vw%26amp;sa%3DD%26amp;ust%3D1534302195679000&sa=D&ust=1534302195779000&usg=AFQjCNHvXLh_twJhq7-ZIaOWGzHqSURz2w)
3. Username enumeration - [https://www.youtube.com/watch?v=WCO7LnSlskE](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DWCO7LnSlskE%26amp;sa%3DD%26amp;ust%3D1534302195679000&sa=D&ust=1534302195779000&usg=AFQjCNHWzUq-pOzAIRpkEma5ImbatLt1YQ)
4. Username enumeration with bruteforce password attack - [https://www.youtube.com/watch?v=zf3-pYJU1c4](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253Dzf3-pYJU1c4%26amp;sa%3DD%26amp;ust%3D1534302195680000&sa=D&ust=1534302195780000&usg=AFQjCNESuYEcwTO_E_h1i-paXVhBbrRnBQ)
5. Authentication over insecure HTTP protocol - [https://www.youtube.com/watch?v=ueSG7TUqoxk](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DueSG7TUqoxk%26amp;sa%3DD%26amp;ust%3D1534302195680000&sa=D&ust=1534302195780000&usg=AFQjCNH8nEDd1CRP9LPUhmnj2iZpR_eLTQ)
6. Authentication over insecure HTTP protocol - [https://www.youtube.com/watch?v=\_WQe36pZ3mA](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D_WQe36pZ3mA%26amp;sa%3DD%26amp;ust%3D1534302195680000&sa=D&ust=1534302195780000&usg=AFQjCNGn1p0sq5_1vHgWeZKT5nq4-ei7vQ)
7. Forgot password vulnerability - case 1 - [https://www.youtube.com/watch?v=FEUidWWnZwU](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DFEUidWWnZwU%26amp;sa%3DD%26amp;ust%3D1534302195681000&sa=D&ust=1534302195780000&usg=AFQjCNFGzL1-dXEKw8q5sJXMTX2WZf-aWg)
8. Forgot password vulnerability - case 2 - [https://www.youtube.com/watch?v=j7-8YyYdWL4](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253Dj7-8YyYdWL4%26amp;sa%3DD%26amp;ust%3D1534302195681000&sa=D&ust=1534302195780000&usg=AFQjCNFnOcJPCaqGpaUd_B-gHkrV3DZSCg)
9. Login page autocomplete feature enabled - [https://www.youtube.com/watch?v=XNjUfwDmHGc&t=33s](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DXNjUfwDmHGc%2526t%253D33s%26amp;sa%3DD%26amp;ust%3D1534302195682000&sa=D&ust=1534302195780000&usg=AFQjCNHNJQ_-ShMPUU-ehnKhAtayFkJEOg)
10. Testing for weak password policy - [https://www.owasp.org/index.php/Testing\_for\_Weak\_password\_policy\_(OTG-AUTHN-007)](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.owasp.org/index.php/Testing_for_Weak_password_policy_(OTG-AUTHN-007)%26amp;sa%3DD%26amp;ust%3D1534302195682000&sa=D&ust=1534302195780000&usg=AFQjCNFHyCJkEuhbwzzIzEiuV-7jEaoFIQ)
11. 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.

**Phase 8 – Phase 8 - Attacking access controls (IDOR, Priv esc, hidden files and directories)**

**Completely unprotected functionalities**

1. Finding admin panel - [https://www.youtube.com/watch?v=r1k2lgvK3s0](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253Dr1k2lgvK3s0%26amp;sa%3DD%26amp;ust%3D1534302195683000&sa=D&ust=1534302195781000&usg=AFQjCNHSngjuN4P2k_NzmhqXoeZSSq3IPQ)
2. Finding admin panel and hidden files and directories - [https://www.youtube.com/watch?v=Z0VAPbATy1A](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DZ0VAPbATy1A%26amp;sa%3DD%26amp;ust%3D1534302195684000&sa=D&ust=1534302195781000&usg=AFQjCNGTNXEZPbrhGuJw3nRwXxCKqZgIMA)
3. Finding hidden webpages with dirbusater - [https://www.youtube.com/watch?v=--nu9Jq07gA&t=5s](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D--nu9Jq07gA%2526t%253D5s%26amp;sa%3DD%26amp;ust%3D1534302195684000&sa=D&ust=1534302195781000&usg=AFQjCNEs_vSoJpdi0-Upex8gKK24z2by7g)

**Insecure direct object reference**

1. IDOR case 1 - [https://www.youtube.com/watch?v=gci4R9Vkulc](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253Dgci4R9Vkulc%26amp;sa%3DD%26amp;ust%3D1534302195685000&sa=D&ust=1534302195781000&usg=AFQjCNH4XLXZ2wnmoxDydo5Fvq8L1qUPPw)
2. IDOR case 2 - [https://www.youtube.com/watch?v=4DTULwuLFS0](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D4DTULwuLFS0%26amp;sa%3DD%26amp;ust%3D1534302195686000&sa=D&ust=1534302195781000&usg=AFQjCNGObi-VZMz_a0KvF0x4TtDgXEzBrA)
3. IDOR case 3 (zomato) - [https://www.youtube.com/watch?v=tCJBLG5Mayo](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DtCJBLG5Mayo%26amp;sa%3DD%26amp;ust%3D1534302195686000&sa=D&ust=1534302195781000&usg=AFQjCNExKilcYQizgFn-o2aYebdYjn1j0Q)

**Privilege escalation**

1. What is privilege escalation - [https://www.youtube.com/watch?v=80RzLSrczmc](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D80RzLSrczmc%26amp;sa%3DD%26amp;ust%3D1534302195687000&sa=D&ust=1534302195782000&usg=AFQjCNGoc-CMXhOASOI2nXyvMKSjQLV3ZQ)
2. Privilege escalation - Hackme bank - case 1 - [https://www.youtube.com/watch?v=g3lv\_\_87cWM](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253Dg3lv__87cWM%26amp;sa%3DD%26amp;ust%3D1534302195687000&sa=D&ust=1534302195782000&usg=AFQjCNGzDfOHGZSE5XZzecJ-NVsgK4zbMw)
3. Privilege escalation - case 2 - [https://www.youtube.com/watch?v=-i4O\_hjc87Y](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D-i4O_hjc87Y%26amp;sa%3DD%26amp;ust%3D1534302195687000&sa=D&ust=1534302195782000&usg=AFQjCNFFR8Vv9x7K1cXjiNpmREqZBhZdVQ)

**Phase 9 – Attacking data stores (Various types of injection attacks - SQL|MySQL|NoSQL|Oracle, etc.)**

**Bypassing login panel**

1. Basics of MySQL - [https://www.youtube.com/watch?v=yPu6qV5byu4](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DyPu6qV5byu4%26amp;sa%3DD%26amp;ust%3D1534302195688000&sa=D&ust=1534302195782000&usg=AFQjCNFlNHRjSkaYccpR3F4koAta0LX-fQ)
2. Bypassing login panel -case 1 - [https://www.youtube.com/watch?v=TSqXkkOt6oM](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DTSqXkkOt6oM%26amp;sa%3DD%26amp;ust%3D1534302195689000&sa=D&ust=1534302195782000&usg=AFQjCNGuZJSJO39msJ46HJXbNVIEwJD6wg)
3. Bypass login panel - case 2 - [https://www.youtube.com/watch?v=J6v\_W-LFK1c](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DJ6v_W-LFK1c%26amp;sa%3DD%26amp;ust%3D1534302195689000&sa=D&ust=1534302195782000&usg=AFQjCNEzzUMKy9ZMKIoOulIxYgNjET0w7w)

**SQL injection**

1. Part 1 - Install SQLi lab - [https://www.youtube.com/watch?v=NJ9AA1\_t1Ic&index=23&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DNJ9AA1_t1Ic%2526index%253D23%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%26amp;sa%3DD%26amp;ust%3D1534302195690000&sa=D&ust=1534302195783000&usg=AFQjCNGTKGumVl257ZRd8XhiY0hEp8NN1A)
2. Part 2 - SQL lab series - [https://www.youtube.com/watch?v=TA2h\_kUqfhU&index=22&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DTA2h_kUqfhU%2526index%253D22%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%26amp;sa%3DD%26amp;ust%3D1534302195690000&sa=D&ust=1534302195783000&usg=AFQjCNHoyGF6t3n3gT1GnVLmbvmlMoCtRg)
3. Part 3 - SQL lab series - [https://www.youtube.com/watch?v=N0zAChmZIZU&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=21](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DN0zAChmZIZU%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%2526index%253D21%26amp;sa%3DD%26amp;ust%3D1534302195691000&sa=D&ust=1534302195783000&usg=AFQjCNF1a0mEWesii4yHk4n_cAYowsqTrA)
4. Part 4 - SQL lab series - [https://www.youtube.com/watch?v=6pVxm5mWBVU&index=20&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D6pVxm5mWBVU%2526index%253D20%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%26amp;sa%3DD%26amp;ust%3D1534302195691000&sa=D&ust=1534302195783000&usg=AFQjCNGALtU_0TUioi3GeiSNQTCtpjpI2g)
5. Part 5 - SQL lab series - [https://www.youtube.com/watch?v=0tyerVP9R98&index=19&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D0tyerVP9R98%2526index%253D19%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%26amp;sa%3DD%26amp;ust%3D1534302195692000&sa=D&ust=1534302195783000&usg=AFQjCNFgp_rOYiY4DWaNWu0ASRrPZlnDFA)
6. Part 6 - Double query injection - [https://www.youtube.com/watch?v=zaRlcPbfX4M&index=18&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DzaRlcPbfX4M%2526index%253D18%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%26amp;sa%3DD%26amp;ust%3D1534302195692000&sa=D&ust=1534302195783000&usg=AFQjCNG407V-N9qVlrXYBWsw-Mlsb8YO3Q)
7. Part 7 - Double query injection cont.. - [https://www.youtube.com/watch?v=9utdAPxmvaI&index=17&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D9utdAPxmvaI%2526index%253D17%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%26amp;sa%3DD%26amp;ust%3D1534302195693000&sa=D&ust=1534302195783000&usg=AFQjCNHFnwvFazpJyppukVp89Zhki2YOvg)
8. Part 8 - Blind injection boolean based - [https://www.youtube.com/watch?v=u7Z7AIR6cMI&index=16&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253Du7Z7AIR6cMI%2526index%253D16%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%26amp;sa%3DD%26amp;ust%3D1534302195694000&sa=D&ust=1534302195784000&usg=AFQjCNGI2QmP5ck0y0yPd2vSO5typlDkrA)
9. Part 9 - Blind injection time based - [https://www.youtube.com/watch?v=gzU1YBu\_838&index=15&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DgzU1YBu_838%2526index%253D15%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%26amp;sa%3DD%26amp;ust%3D1534302195694000&sa=D&ust=1534302195784000&usg=AFQjCNH-w1Jy3tEA_KdA1acbhh9xXFesAw)
10. Part 10 - Dumping DB using outfile - [https://www.youtube.com/watch?v=ADW844OA6io&index=14&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DADW844OA6io%2526index%253D14%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%26amp;sa%3DD%26amp;ust%3D1534302195695000&sa=D&ust=1534302195784000&usg=AFQjCNFNczddJmXeS7kXapmRxxBE2Eyfdw)
11. Part 11 - Post parameter injection error based - [https://www.youtube.com/watch?v=6sQ23tqiTXY&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=13](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D6sQ23tqiTXY%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%2526index%253D13%26amp;sa%3DD%26amp;ust%3D1534302195695000&sa=D&ust=1534302195784000&usg=AFQjCNHo3vnuXyjIp-d80xlaCLIRti8XEQ)
12. Part 12 - POST parameter injection double query based - [https://www.youtube.com/watch?v=tjFXWQY4LuA&index=12&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DtjFXWQY4LuA%2526index%253D12%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%26amp;sa%3DD%26amp;ust%3D1534302195695000&sa=D&ust=1534302195784000&usg=AFQjCNHhZ7TfYI5IX1mRHVay_xtFdudiRA)
13. Part 13 - POST parameter injection blind boolean and time based - [https://www.youtube.com/watch?v=411G-4nH5jE&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=10](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D411G-4nH5jE%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%2526index%253D10%26amp;sa%3DD%26amp;ust%3D1534302195696000&sa=D&ust=1534302195784000&usg=AFQjCNESOZxzOXofaWRGhG3qi_fACyuxIA)
14. Part 14 - Post parameter injection in UPDATE query - [https://www.youtube.com/watch?v=2FgLcPuU7Vw&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=11](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D2FgLcPuU7Vw%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%2526index%253D11%26amp;sa%3DD%26amp;ust%3D1534302195697000&sa=D&ust=1534302195785000&usg=AFQjCNF72Vxfs0H7uiW5HT-oqUxC-3hgXg)
15. Part 15 - Injection in insert query - [https://www.youtube.com/watch?v=ZJiPsWxXYZs&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=9](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DZJiPsWxXYZs%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%2526index%253D9%26amp;sa%3DD%26amp;ust%3D1534302195697000&sa=D&ust=1534302195785000&usg=AFQjCNFzLCK6ZDbUyHPN3FH1idx5EOvmwQ)
16. Part 16 - Cookie based injection - [https://www.youtube.com/watch?v=-A3vVqfP8pA&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=8](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D-A3vVqfP8pA%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%2526index%253D8%26amp;sa%3DD%26amp;ust%3D1534302195698000&sa=D&ust=1534302195785000&usg=AFQjCNFYQ1pjZRgx4-R3Rmno_RjGV5EOkQ)
17. Part 17 - Second order injection  -[https://www.youtube.com/watch?v=e9pbC5BxiAE&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=7](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253De9pbC5BxiAE%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%2526index%253D7%26amp;sa%3DD%26amp;ust%3D1534302195698000&sa=D&ust=1534302195785000&usg=AFQjCNHg-XqKY8YcRvdGMuVkooLrQx8Rcw)
18. Part 18 - Bypassing blacklist filters - 1 - [https://www.youtube.com/watch?v=5P-knuYoDdw&index=6&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D5P-knuYoDdw%2526index%253D6%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%26amp;sa%3DD%26amp;ust%3D1534302195699000&sa=D&ust=1534302195785000&usg=AFQjCNFtF2hXrw6kKsSC45yP5RriUHvSSQ)
19. Part 19 - Bypassing blacklist filters - 2 - [https://www.youtube.com/watch?v=45BjuQFt55Y&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=5](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D45BjuQFt55Y%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%2526index%253D5%26amp;sa%3DD%26amp;ust%3D1534302195699000&sa=D&ust=1534302195785000&usg=AFQjCNHTLLkuCEU4KiJOUoLtiSrKIDDDlA)
20. Part 20 - Bypassing blacklist filters  - 3 - [https://www.youtube.com/watch?v=c-Pjb\_zLpH0&index=4&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253Dc-Pjb_zLpH0%2526index%253D4%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%26amp;sa%3DD%26amp;ust%3D1534302195700000&sa=D&ust=1534302195785000&usg=AFQjCNHZyFRxdztwlCNlArc8o7psHzHD4w)
21. Part 21 - Bypassing WAF - [https://www.youtube.com/watch?v=uRDuCXFpHXc&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=2](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DuRDuCXFpHXc%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%2526index%253D2%26amp;sa%3DD%26amp;ust%3D1534302195700000&sa=D&ust=1534302195786000&usg=AFQjCNGdrYoN06HXddSykfAMW82upSjVEg)
22. Part 22 - Bypassing WAF - Impedance mismatch - [https://www.youtube.com/watch?v=ygVUebdv\_Ws&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=3](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DygVUebdv_Ws%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%2526index%253D3%26amp;sa%3DD%26amp;ust%3D1534302195701000&sa=D&ust=1534302195786000&usg=AFQjCNHA8N3spwcm1ZIMlmhXC9i01eVwRw)
23. Part 23 - Bypassing addslashes - charset mismatch - [https://www.youtube.com/watch?v=du-jkS6-sbo&list=PLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro&index=1](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253Ddu-jkS6-sbo%2526list%253DPLkiAz1NPnw8qEgzS7cgVMKavvOAdogsro%2526index%253D1%26amp;sa%3DD%26amp;ust%3D1534302195701000&sa=D&ust=1534302195786000&usg=AFQjCNECgZxQpf2rIAqvddvMy6FAPeuoNg)

**NoSQL injection**

1. Abusing NoSQL databases - [https://www.youtube.com/watch?v=lcO1BTNh8r8](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DlcO1BTNh8r8%26amp;sa%3DD%26amp;ust%3D1534302195702000&sa=D&ust=1534302195786000&usg=AFQjCNHpXXMWyqWEbOf0JrgzK6iqv00o1A)
2. Making cry - attacking NoSQL for pentesters - [https://www.youtube.com/watch?v=NgsesuLpyOg](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DNgsesuLpyOg%26amp;sa%3DD%26amp;ust%3D1534302195703000&sa=D&ust=1534302195786000&usg=AFQjCNFTkfX2uQgmKmWXswJAHdRkrr7sSQ)

**Xpath injection**

1. Detailed introduction - [https://www.youtube.com/watch?v=2\_UyM6Ea0Yk&t=3102s](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D2_UyM6Ea0Yk%2526t%253D3102s%26amp;sa%3DD%26amp;ust%3D1534302195703000&sa=D&ust=1534302195787000&usg=AFQjCNGC9mSKbWI9Md4wdfXUS0-NjgVg9w)
2. Practical 1 - bWAPP - [https://www.youtube.com/watch?v=6tV8EuaHI9M](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D6tV8EuaHI9M%26amp;sa%3DD%26amp;ust%3D1534302195704000&sa=D&ust=1534302195787000&usg=AFQjCNFqQchZd3gUXjD3Knpy5O4TzPa1_g)
3. Practical 2 - Mutillidae - [https://www.youtube.com/watch?v=fV0qsqcScI4](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DfV0qsqcScI4%26amp;sa%3DD%26amp;ust%3D1534302195704000&sa=D&ust=1534302195787000&usg=AFQjCNFwiHO_WynsFuBZJi3P3CUapw3uuw)
4. Practical 3 - webgoat - [https://www.youtube.com/watch?v=5ZDSPVp1TpM](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D5ZDSPVp1TpM%26amp;sa%3DD%26amp;ust%3D1534302195705000&sa=D&ust=1534302195787000&usg=AFQjCNGha5MR6y5Qob8dIEPGkAyp8h5l7Q)

**LDAP injection**

1. Introduction and practical 1 - [https://www.youtube.com/watch?v=-TXFlg7S9ks](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253D-TXFlg7S9ks%26amp;sa%3DD%26amp;ust%3D1534302195705000&sa=D&ust=1534302195787000&usg=AFQjCNH-H0k61ffRYgjVilpt3uFPgH-fYg)
2. Practical 2 - [https://www.youtube.com/watch?v=wtahzm\_R8e4](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253Dwtahzm_R8e4%26amp;sa%3DD%26amp;ust%3D1534302195705000&sa=D&ust=1534302195787000&usg=AFQjCNHvYQS9h_wRI_xQrcPSwWi4z4hEyw)

**Phase 10 – Attacking back-end components (OS command injection, XMl interpreters, mail services, etc.)**

**OS command injection**

1. OS command injection in bWAPP - [https://www.youtube.com/watch?v=qLIkGJrMY9k](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://www.youtube.com/watch?v%253DqLIkGJrMY9k%26amp;sa%3DD%26amp;ust%3D1534302195706000&sa=D&ust=1534302195787000&usg=AFQjCNEKWkhTHHgV9-tCL5ad3LXrFxpN8w)