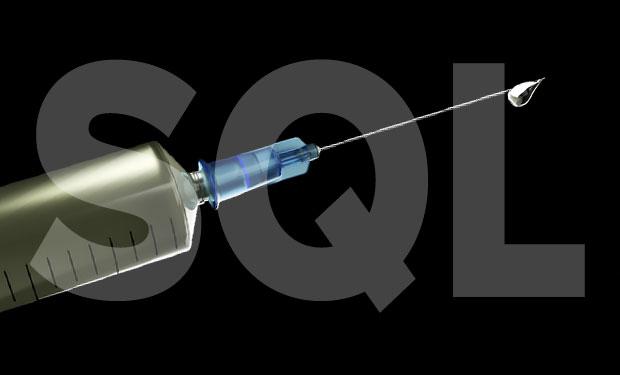
## **SQL Injection Report - OWASP DVWA**



By

RAJAN NISARGAN

### 

### **1. Introduction**

This report details the SQL Injection attack performed on OWASP DVWA, a deliberately vulnerable web application designed to test and enhance web application security skills. The assessment aimed to identify SQL Injection vulnerabilities within the application, exploit them, and provide recommendations for remediation.

### **2. Target Application**

* **Application Name:** OWASP BWA DVWA
* **Testing Tool:** Browser, Burp Suite

### **3. Objective**

The objective of this assessment was to detect SQL Injection vulnerabilities present within the OWASP DVWA application and demonstrate how attackers could exploit these vulnerabilities to extract sensitive information from the database.

### **4. Attack Scenario**

* **Page Targeted:** Login Page
* **Parameter Targeted:** Username / Password Fields
* **Type of Injection:** Authentication Bypass using SQL Injection

### 

### 

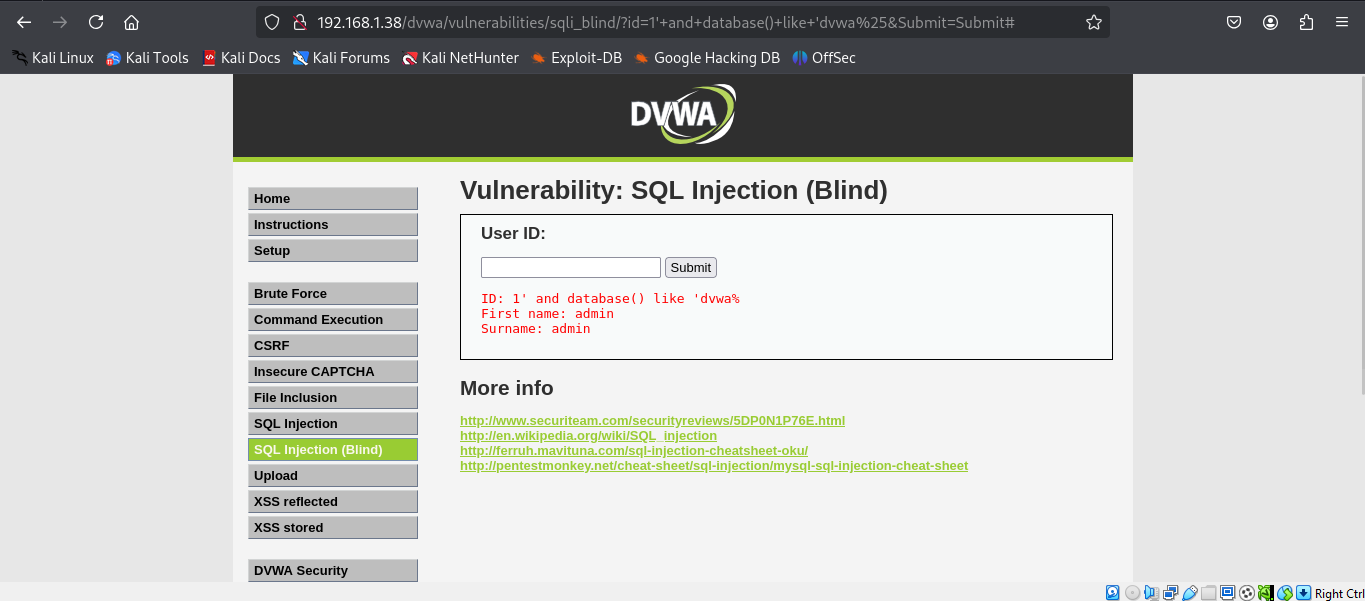
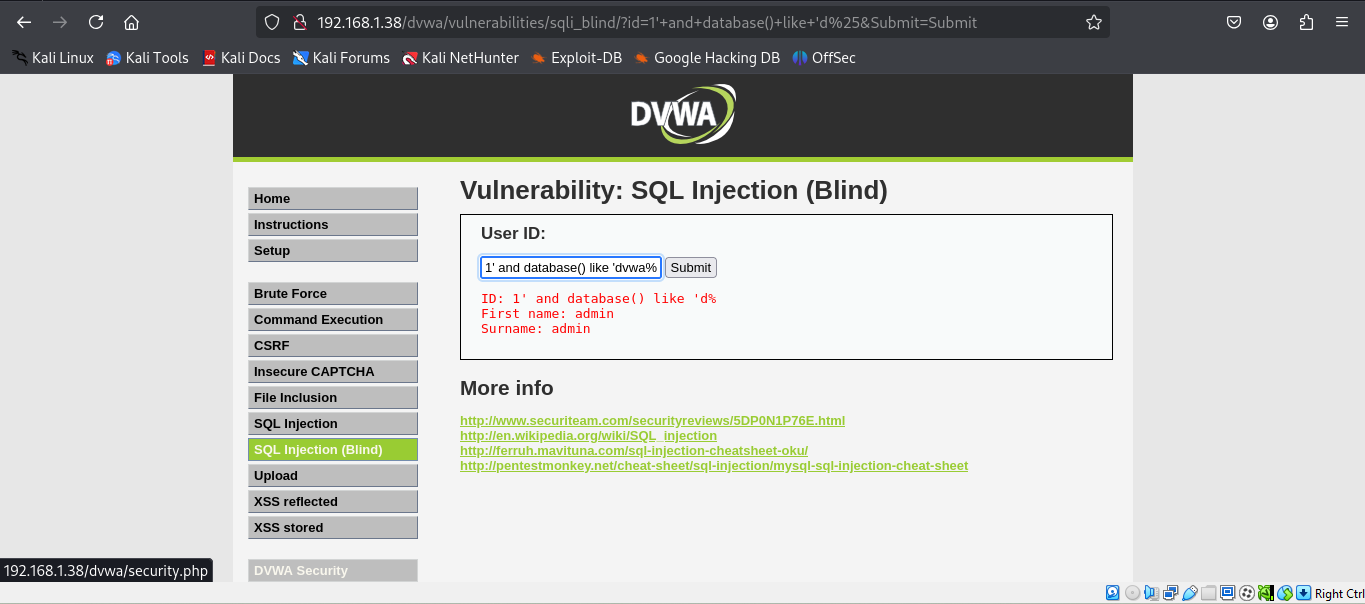
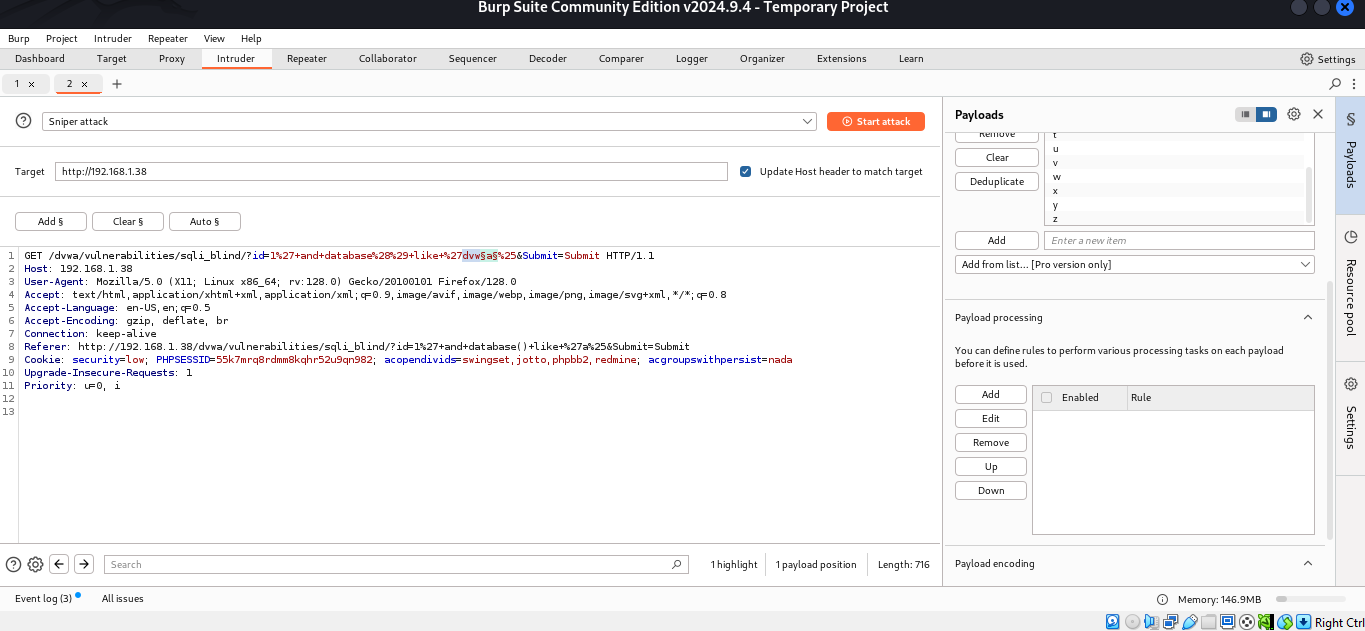
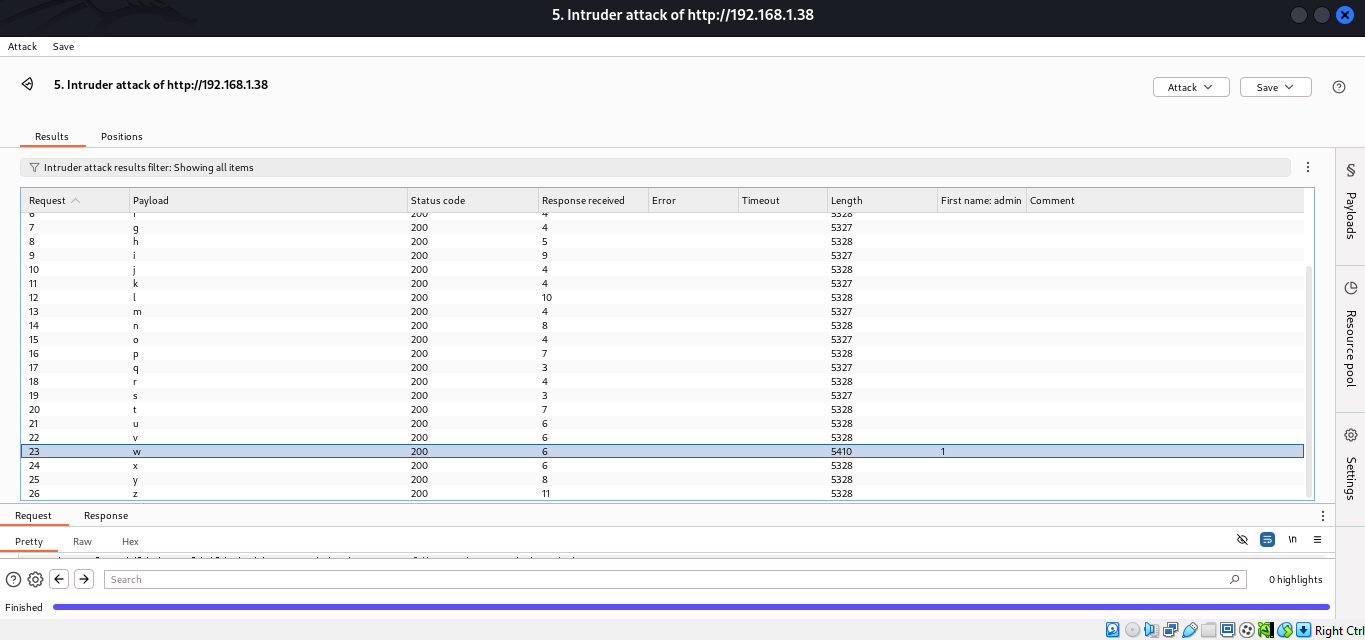
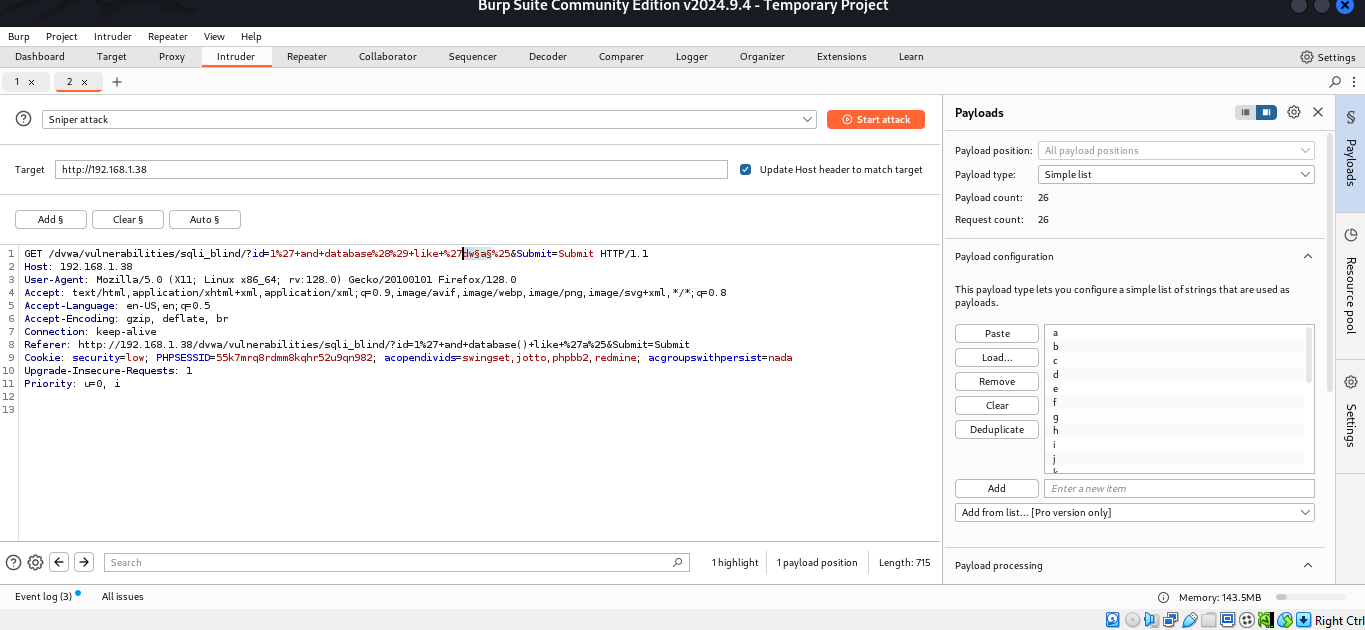
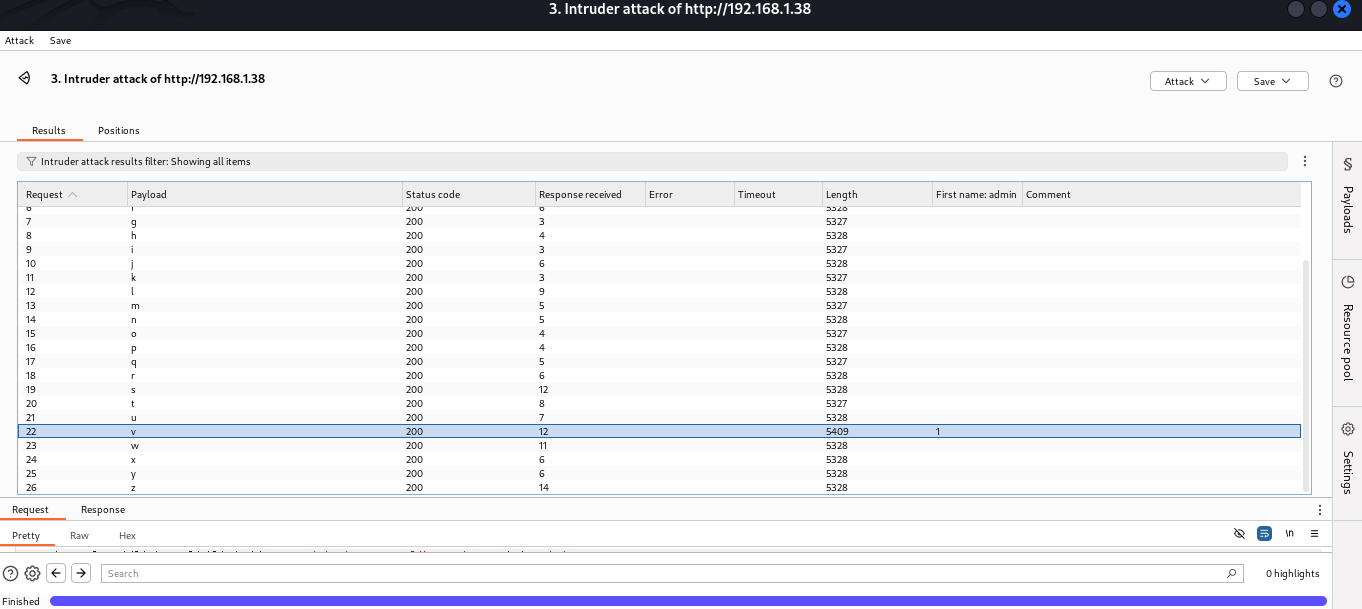
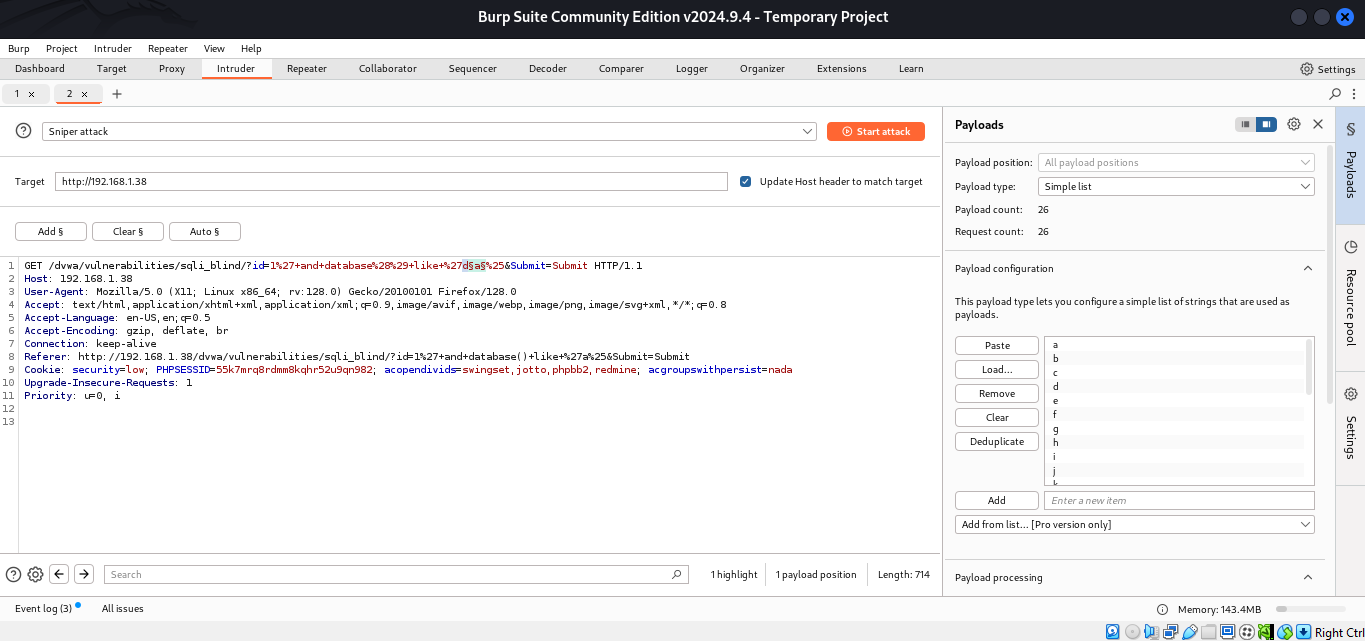
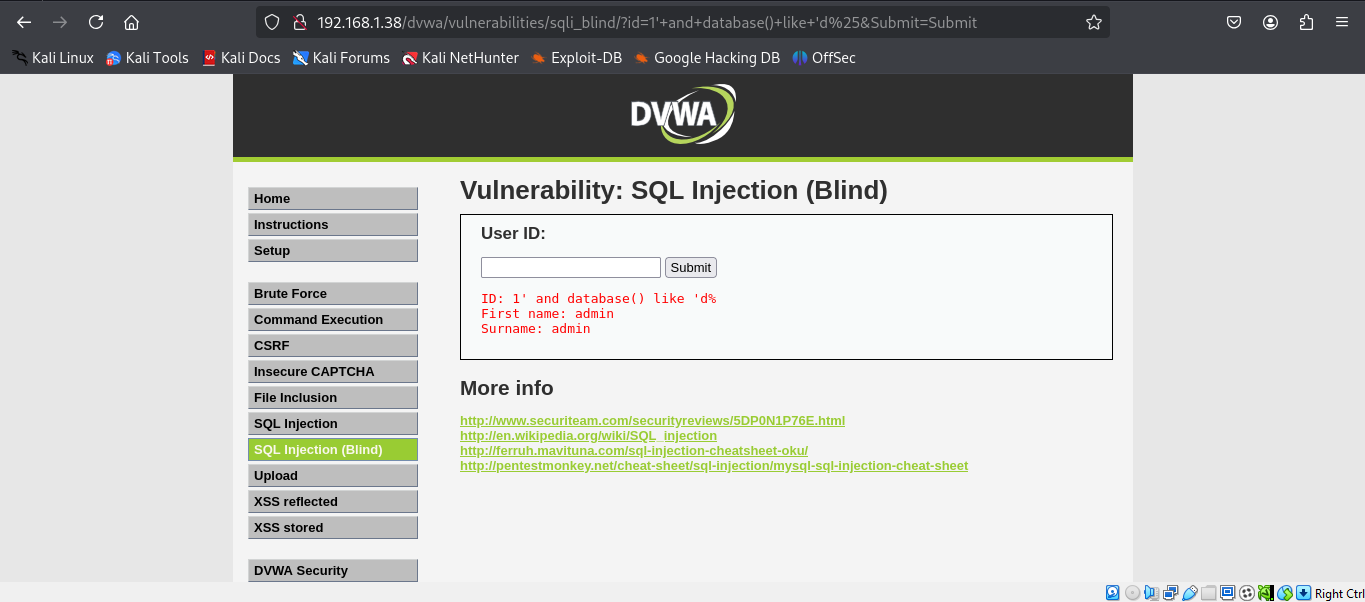
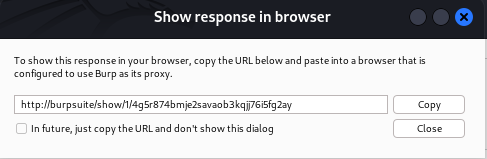
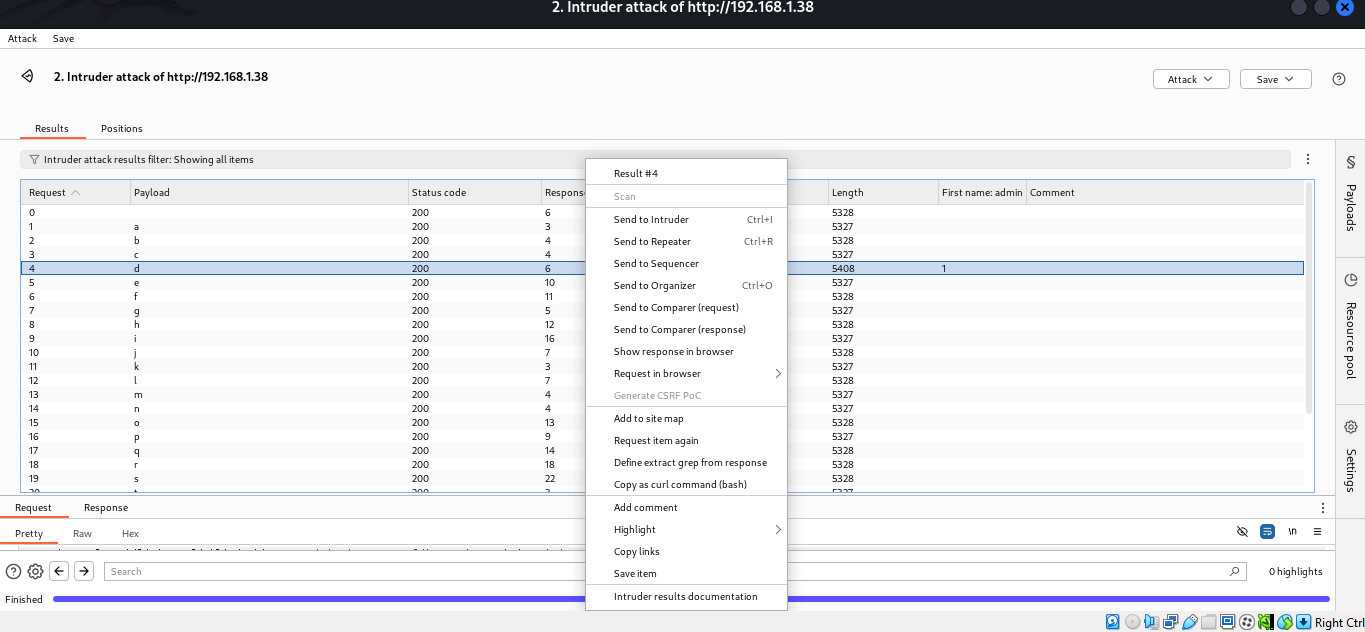
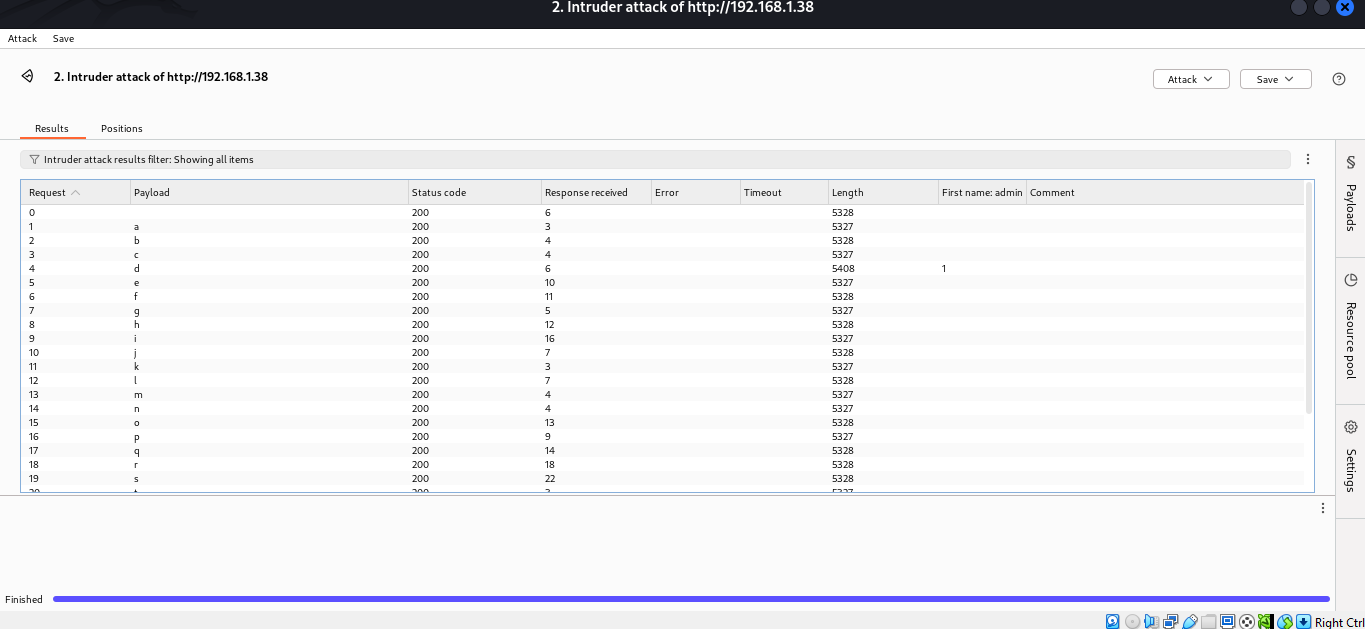
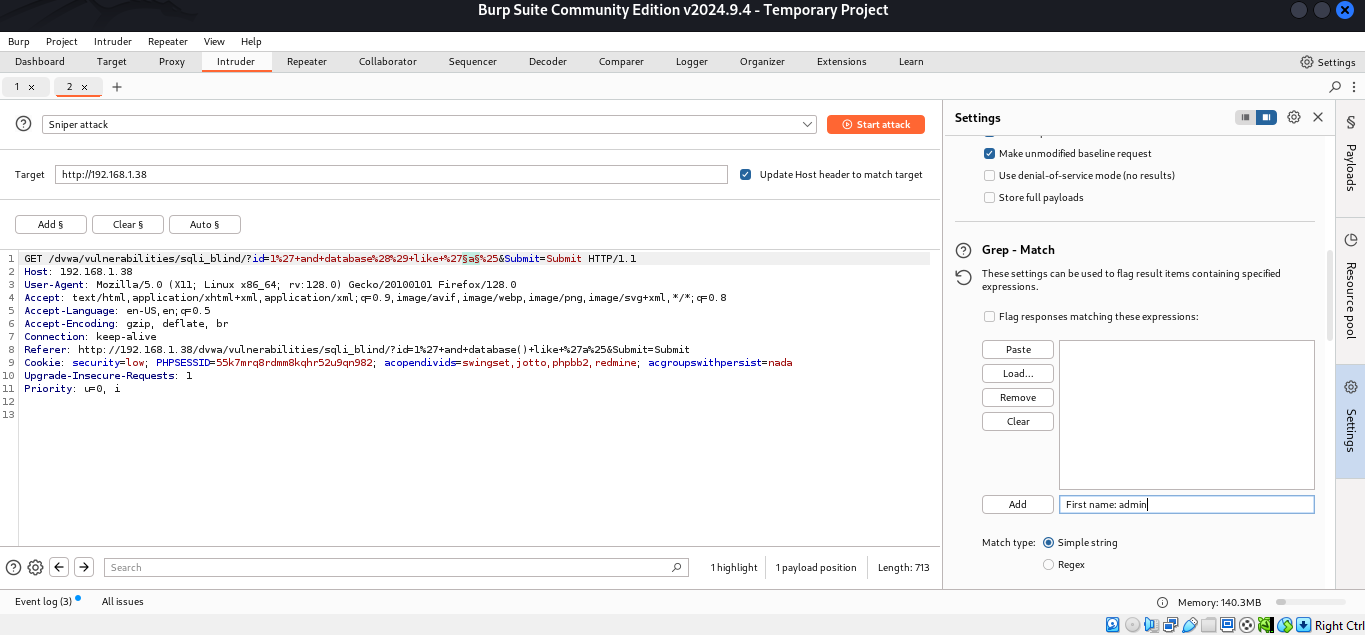
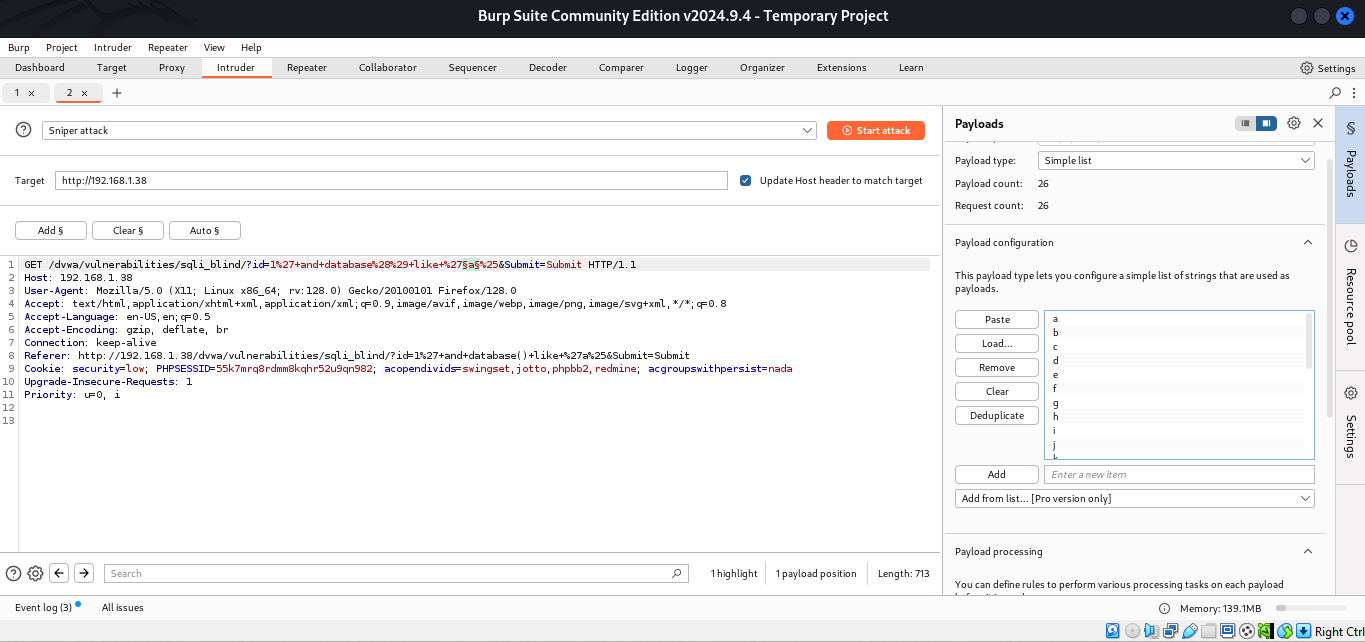
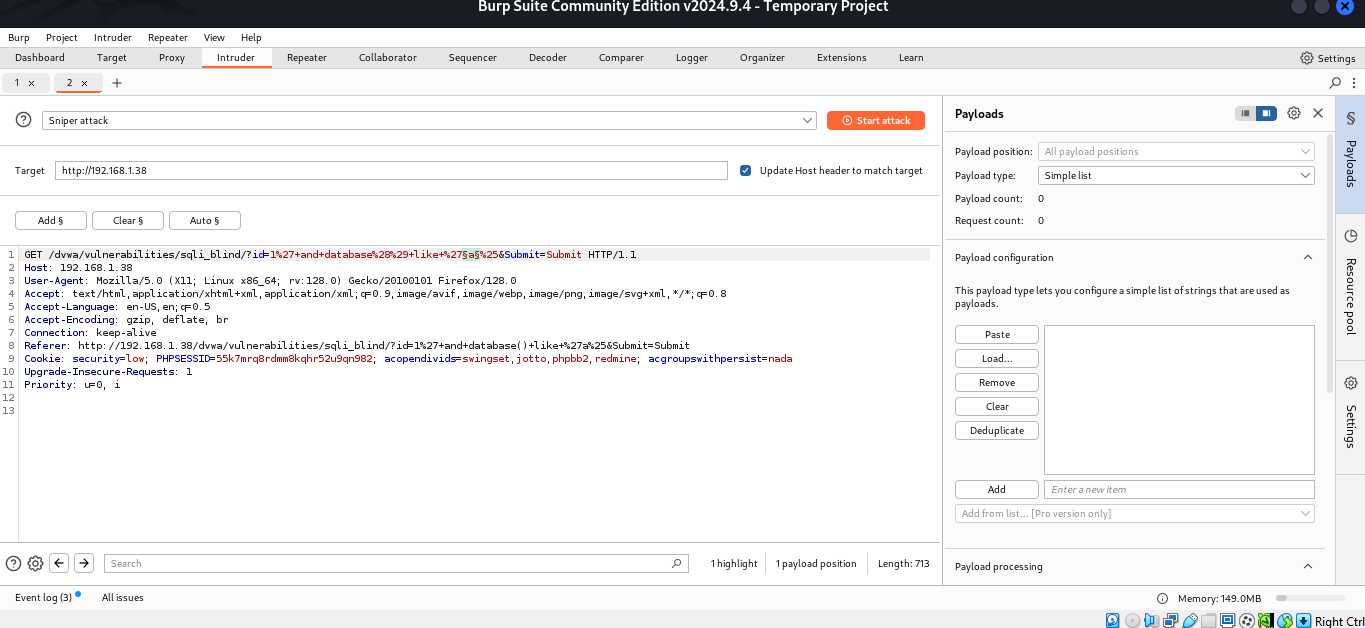
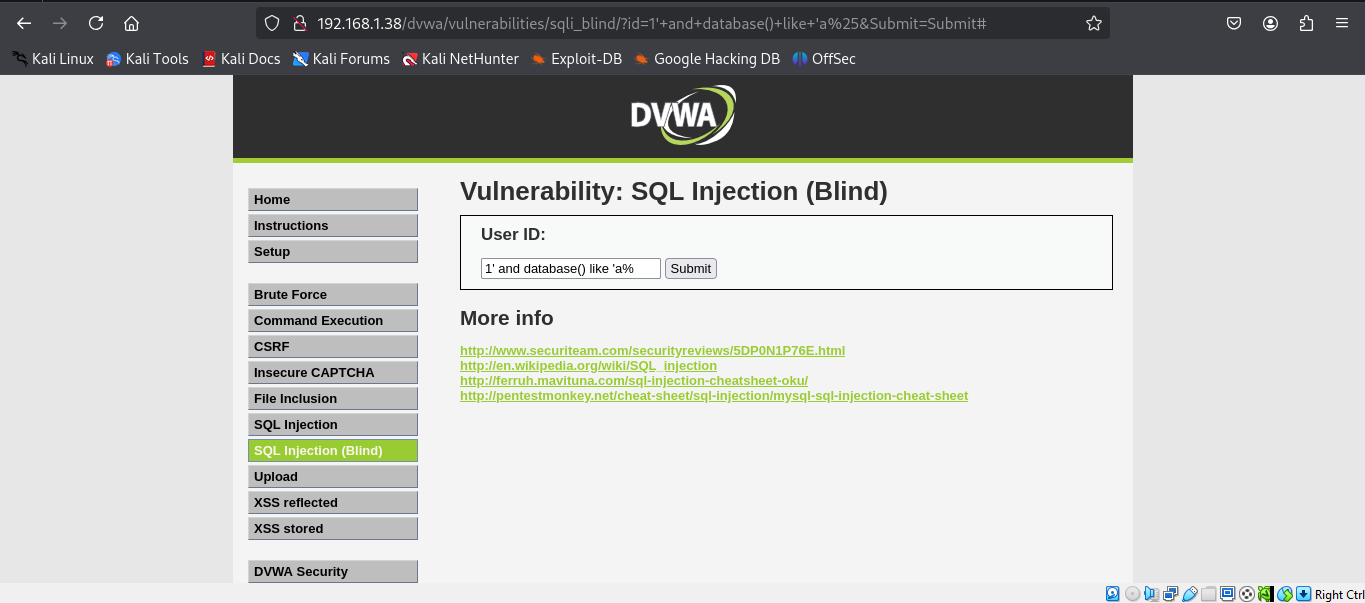
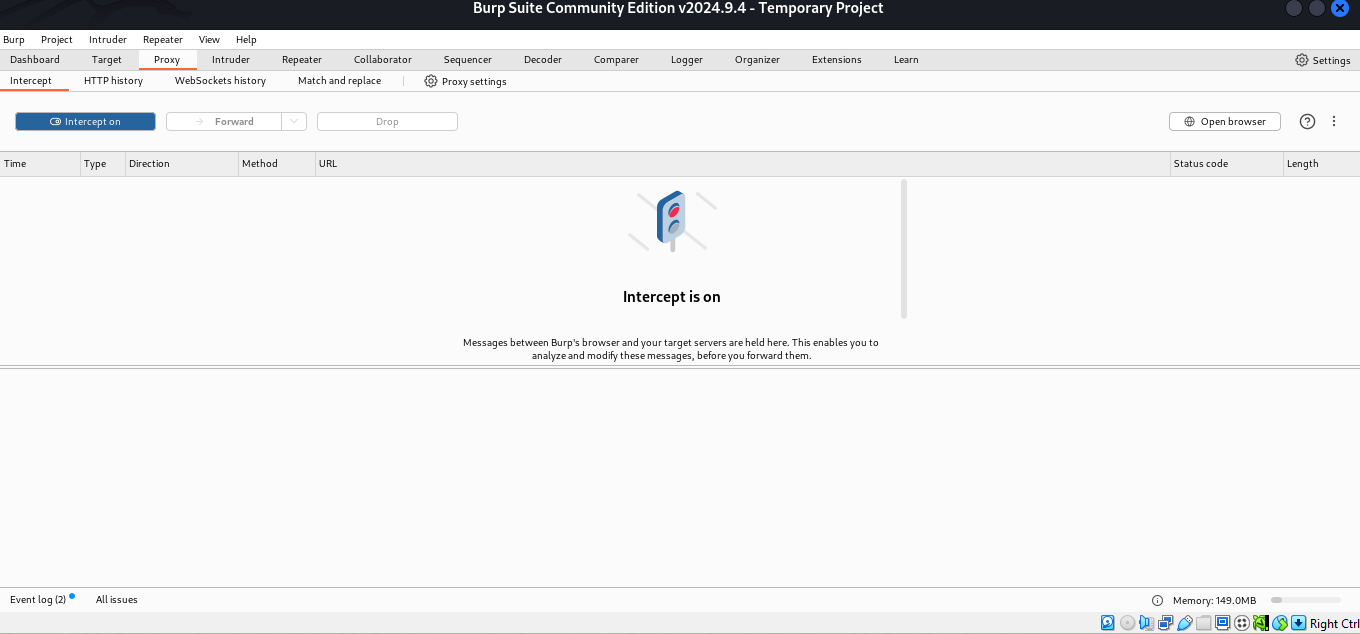
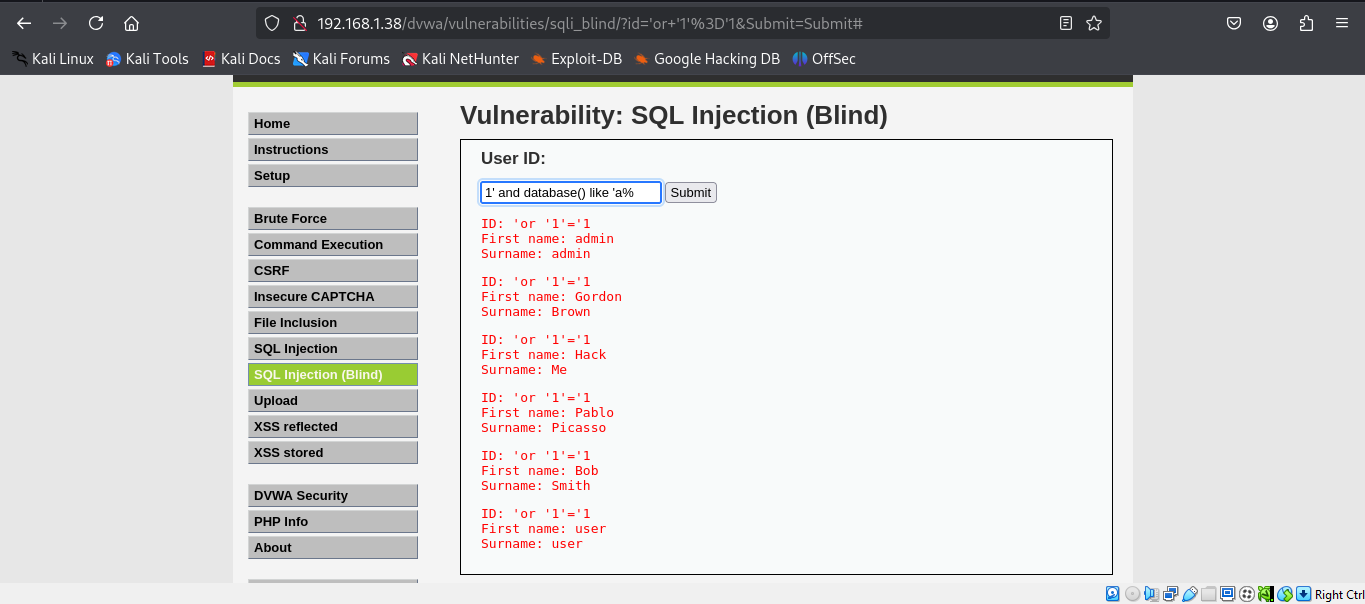
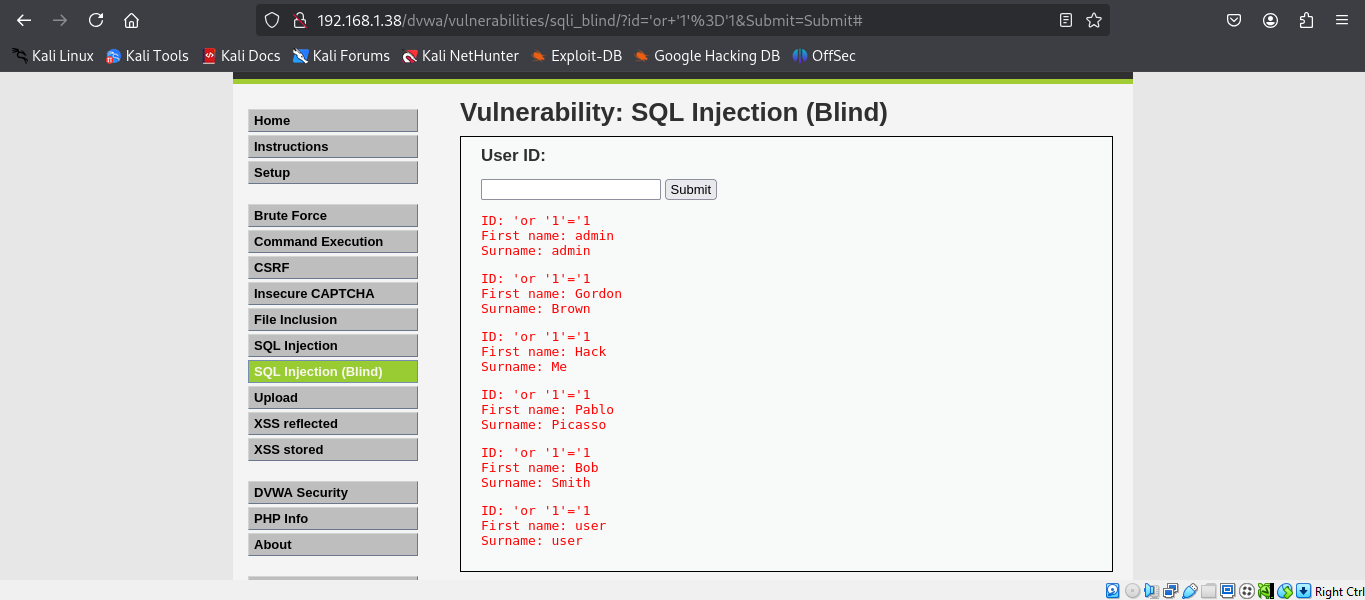
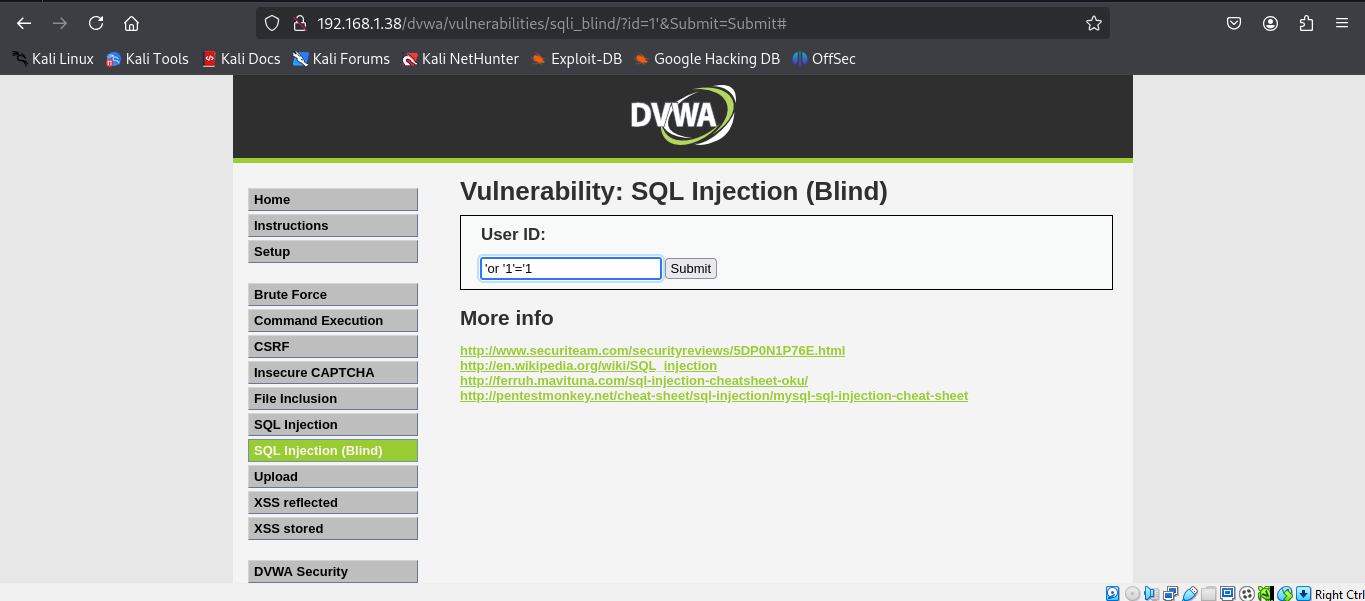
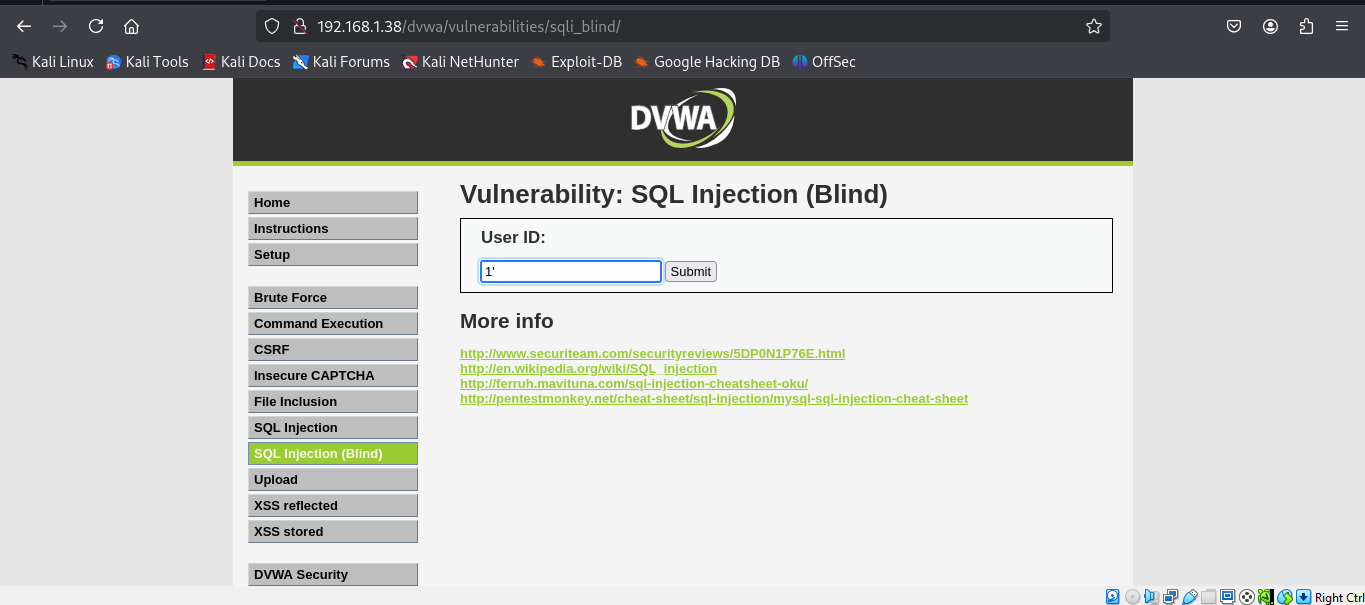
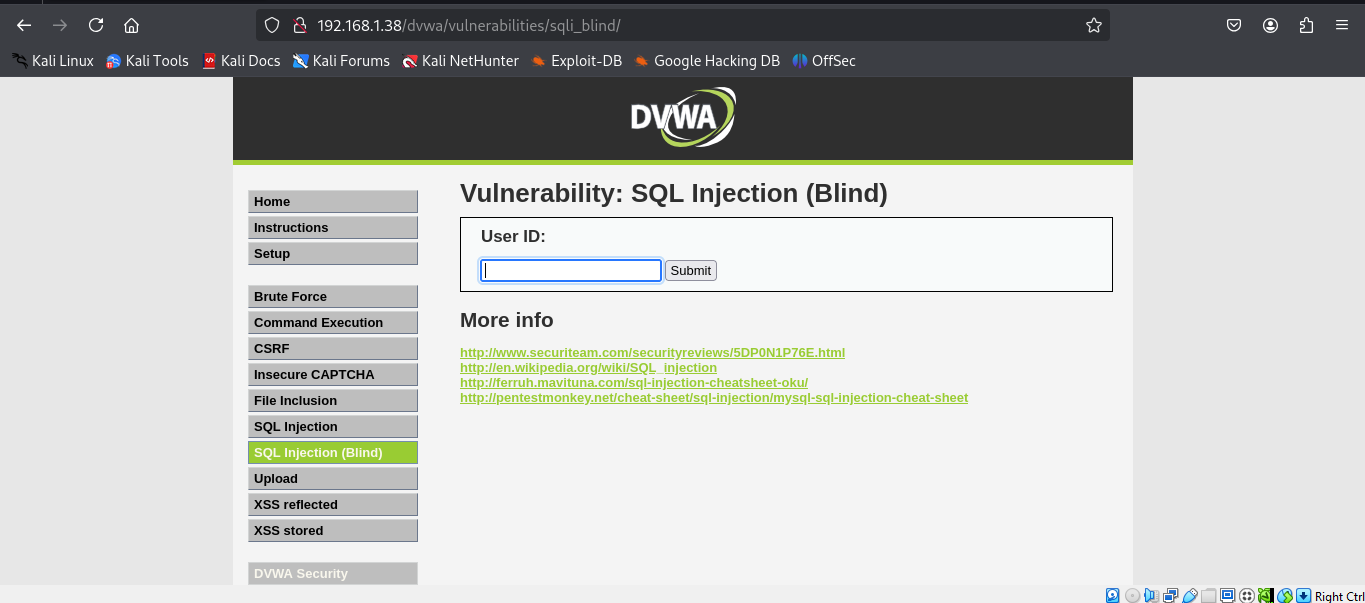
### 

### 

### 

### 

### **5. Steps Performed**



### **6. Impact**

* **Authentication Bypass:** Attackers can gain unauthorized access to sensitive areas of the application.
* **Database Information Disclosure:** Database version and schema details were extracted.
* **Data Exfiltration:** Potential risk of extracting sensitive data from various tables.

### **7. Mitigation Recommendations**

* Implement prepared statements and parameterized queries.
* Use stored procedures instead of dynamic SQL queries.
* Implement robust input validation and sanitization mechanisms.
* Apply the principle of least privilege to database accounts.
* Regularly update and patch software to fix known vulnerabilities.
* Perform regular vulnerability assessments and penetration testing.

### **8. Conclusion**

The assessment successfully demonstrated an SQL Injection vulnerability within the OWASP DVWA application. Proper remediation techniques have been recommended to mitigate this vulnerability.

### **9. References**

* OWASP SQL Injection Prevention Cheat Sheet
* OWASP Mutillidae Documentation