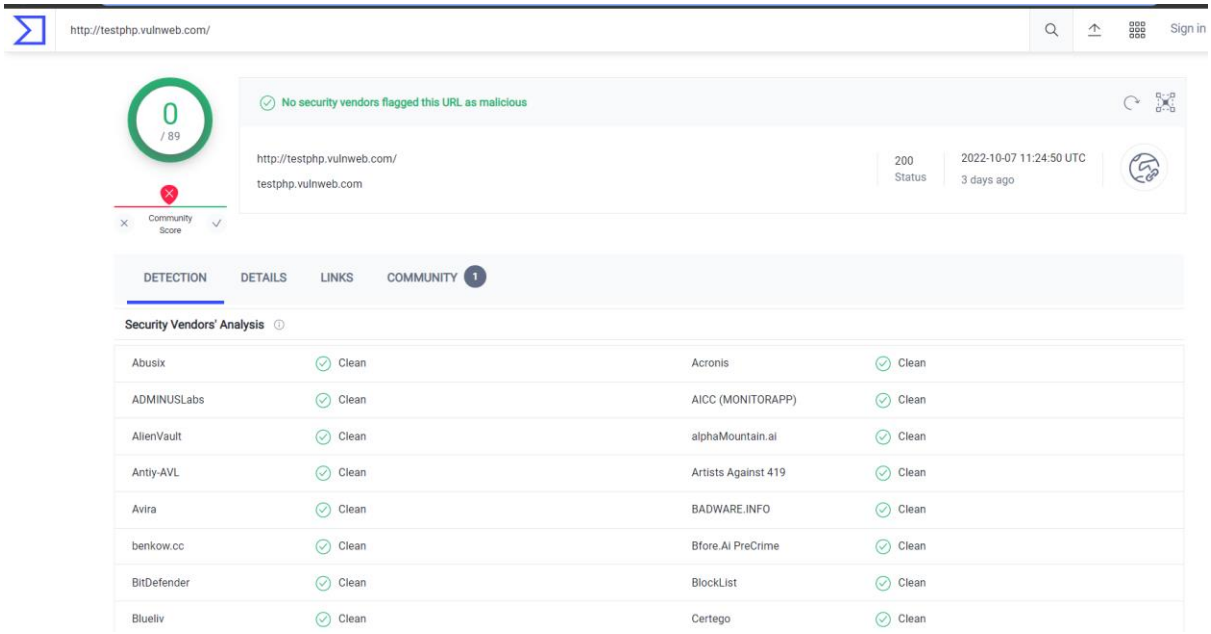
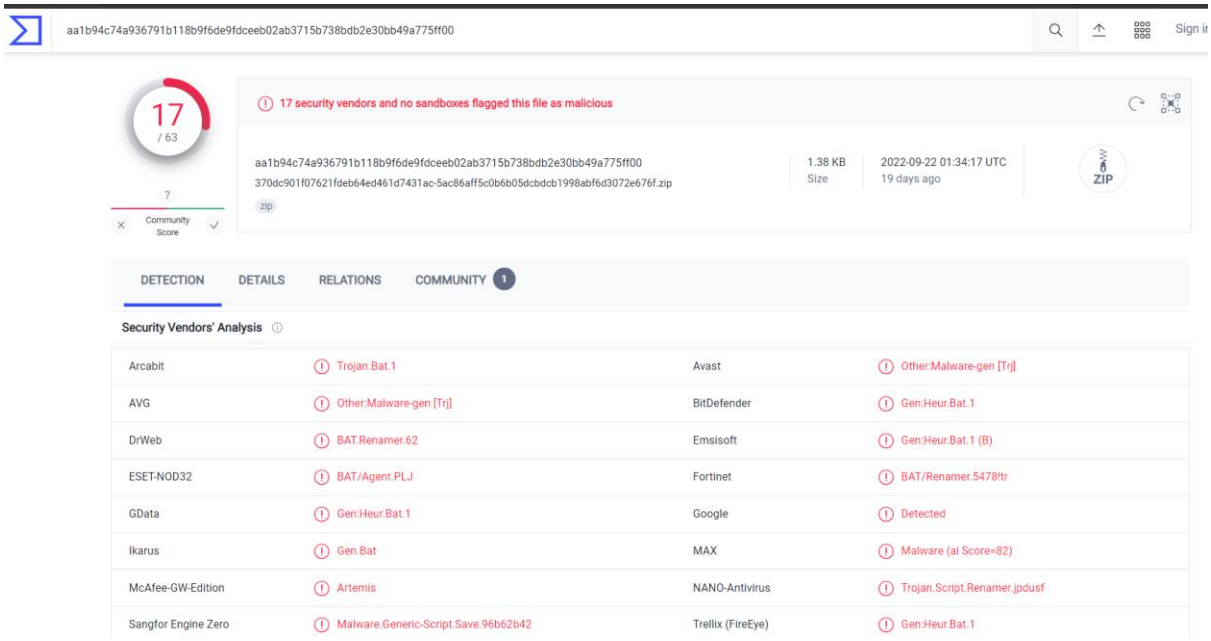
EXPERIMENT 04

VIRUSTOTAL :

Not Vulnerable :



Vulnerable:



Netsparker:

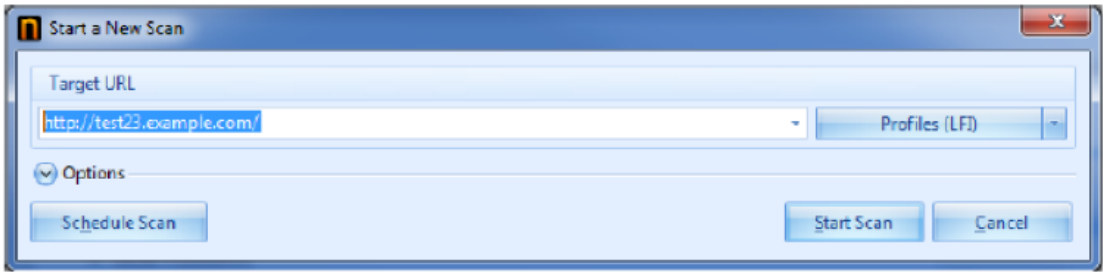
Sample Usages:

Scan `http://test23.example.com` and save the report to `C:\reports\report.pdf`.

```
Netsparker /a /url http://test23.example.com /rf pdf /r C:\reports\scanreport.
pdf
```

Launch a new scan parameter with a custom profile and URL:

```
Netsparker /url http://test23.example.com /p LFI
```



SQL INJECTION:

You can exploit the Error Based or Boolean Based SQL Injection vulnerabilities identified in the web application and run custom SQL queries in the application's database via Netsparker's SQL Injection panel.

From the issues in the Issues panel choose a confirmed "SQL Injection" or "Boolean Based SQL Injection" issue, click the Execute SQL Commands button and the SQL Injection panel will appear where you can run custom SQL queries.

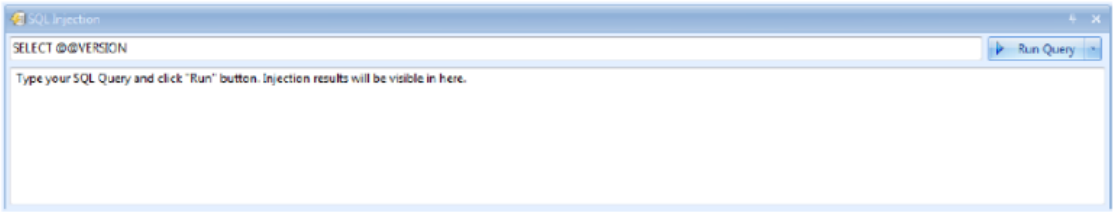


Fig: Running Custom SQL Queries in SQL Injection Panel

Afterwards, you can type an SQL query and run the query with the **Run Query** button. Response of the query will be displayed in the panel.

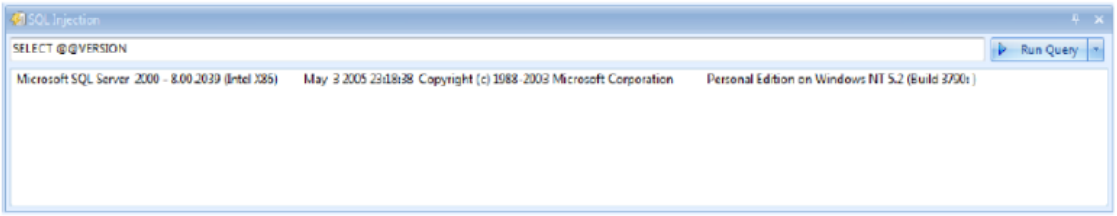


Fig:Sample Custom SQL Query Output