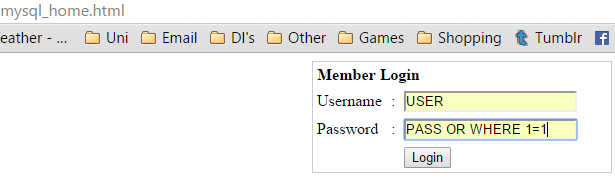
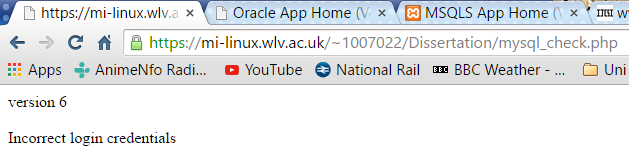
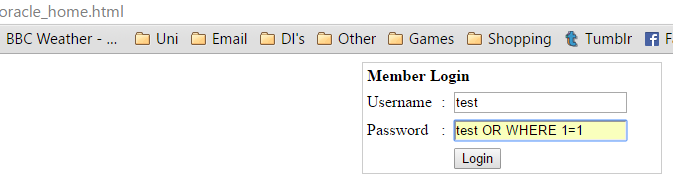
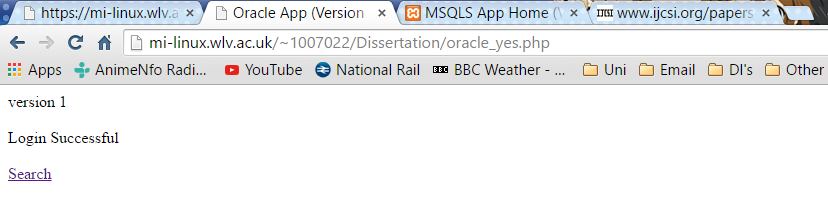
**7ET023 Dissertation appendices**

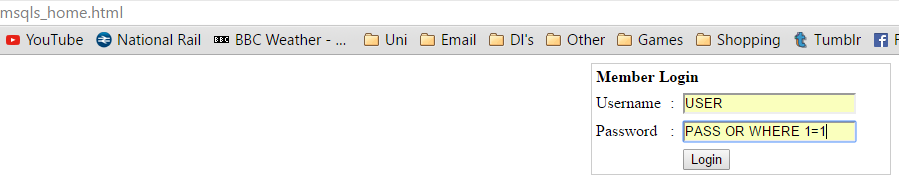
Artefact:

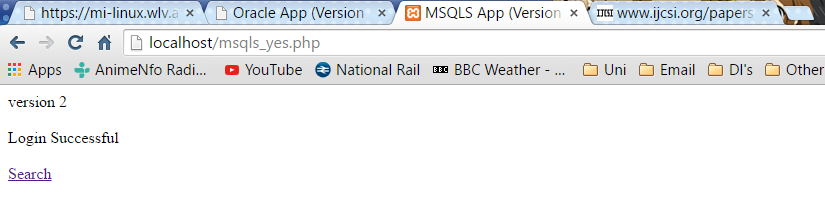
1a) MySQL tautology attack

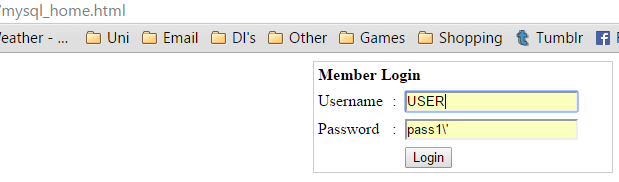
1b) MySQL tautology attack results

1c) Oracle tautology attack

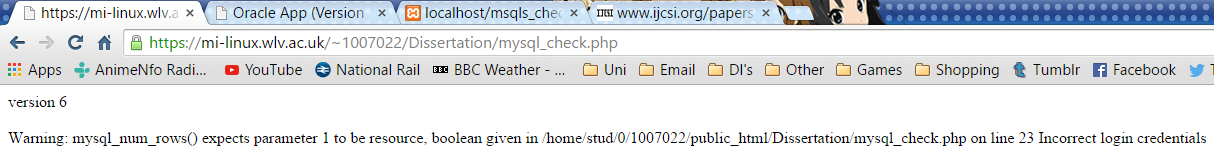
1d) Oracle tautology attack results

1e) MSQLS tautology attack

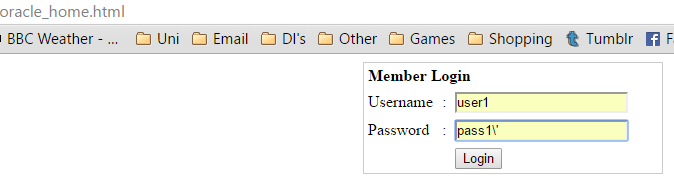
1f) MSQLS tautology attack results

2a) MySQL Illegal/Logically Incorrect Queries attack

2b) MySQL Illegal/Logically Incorrect Queries attack results

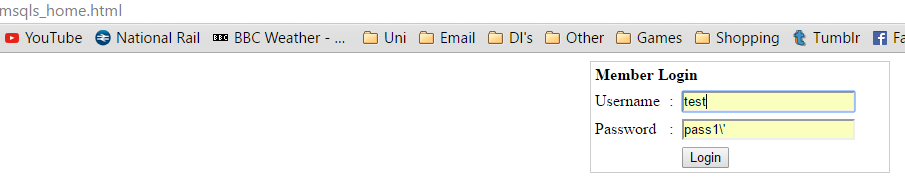


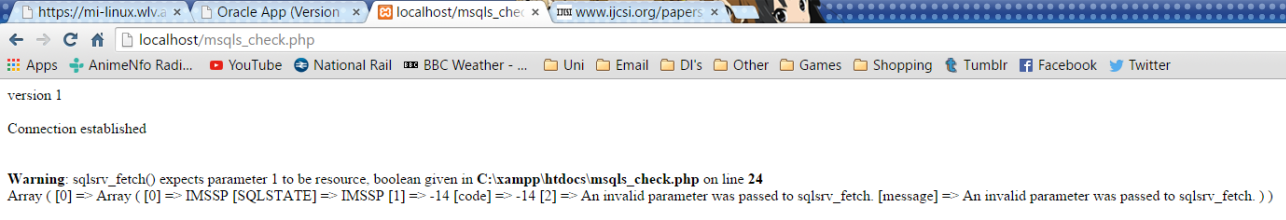
2c) Oracle Illegal/Logically Incorrect Queries attack

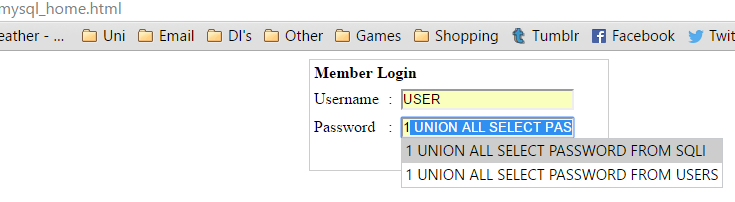


2d) Oracle Illegal/Logically Incorrect Queries attack results

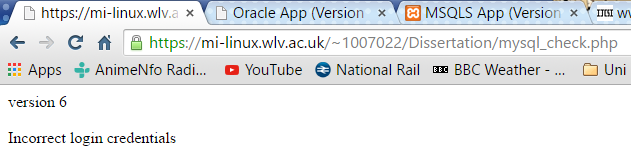


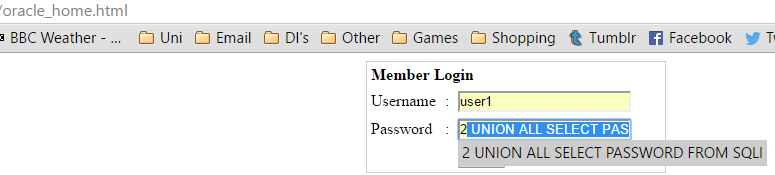
2e) MSQLS Illegal/Logically Incorrect Queries attack

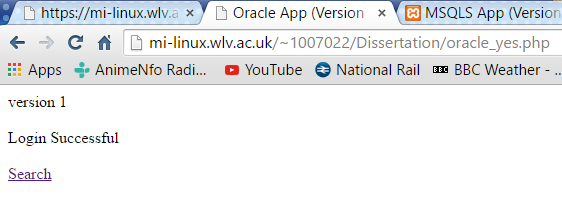
2f) MSQLS Illegal/Logically Incorrect Queries attack results

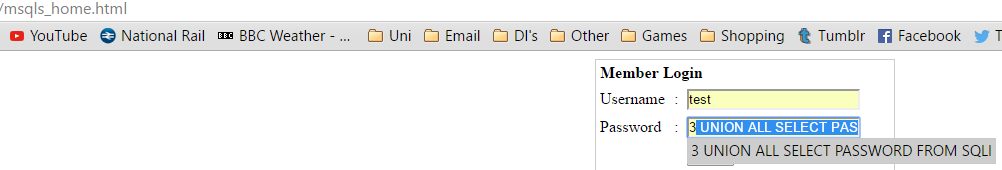


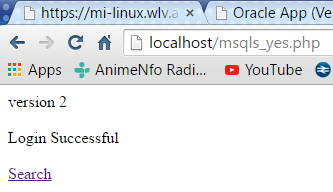
3a) MySQL Union Query attack

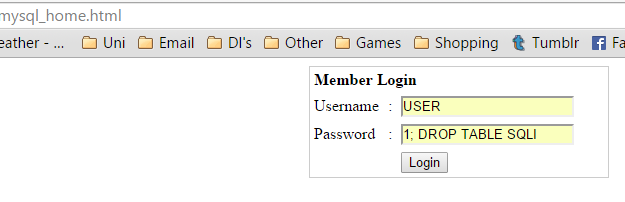
3b) MySQL Union Query attack results

3c) Oracle Union Query attack

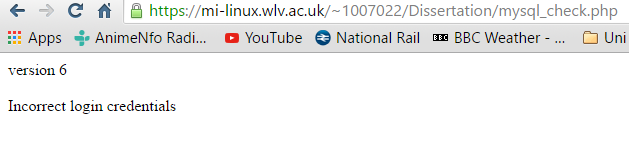
3d) Oracle Union Query attack results

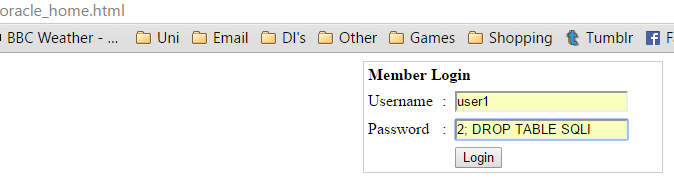
3e) MSQLS Union Query attack

3f) MSQLS Union Query attack results

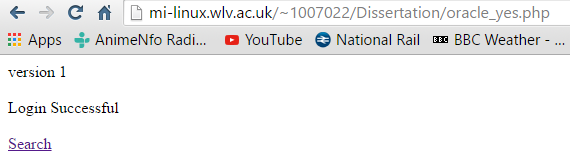
4a) MySQL Piggy-backed Queries attack

4b) MySQL Piggy-backed Queries attack results

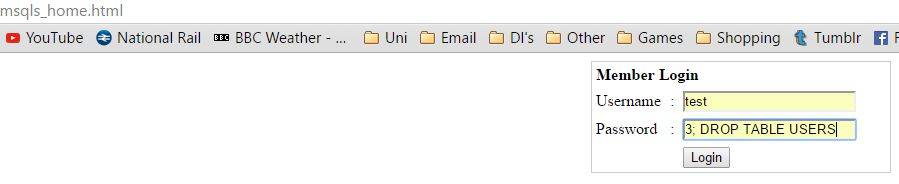


4c) Oracle Piggy-backed Queries attack

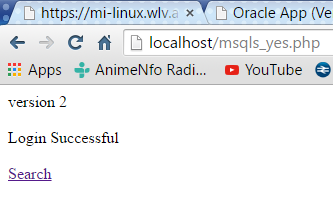
4d) Oracle Piggy-backed Queries attack results



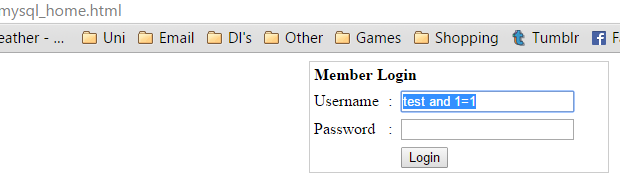
4e) MSQLS Piggy-backed Queries attack

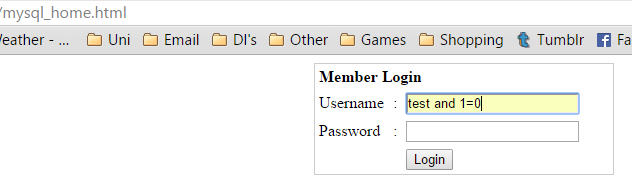


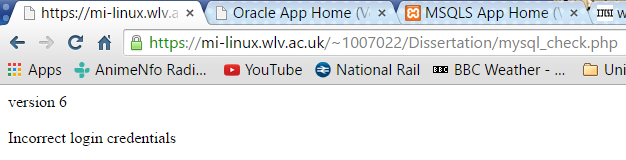
4f) MSQLS Piggy-backed Queries attack results



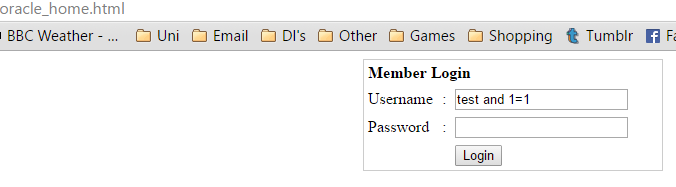
5a) MySQL Blind Injection attack

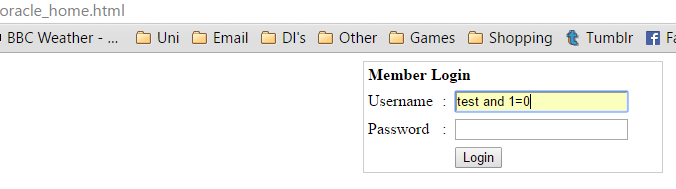




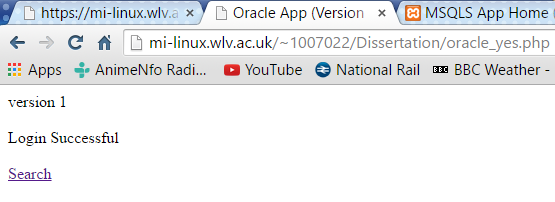
5b) MySQL Blind Injection attack results 

5c) Oracle Blind Injection attack

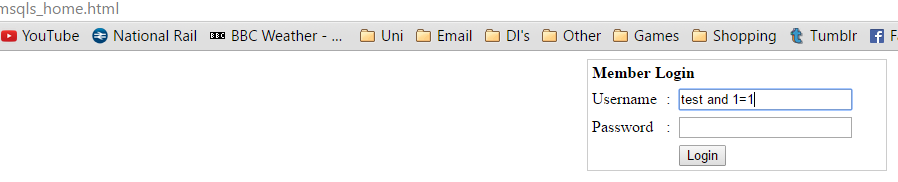


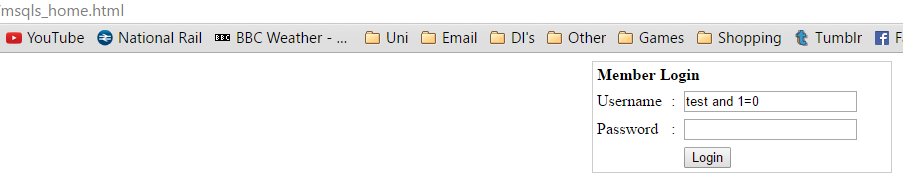


5d) Oracle Blind Injection attack results

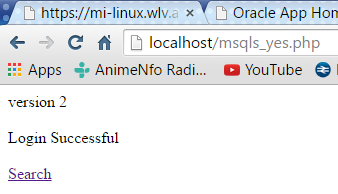


5e) MSQLS Blind Injection attack

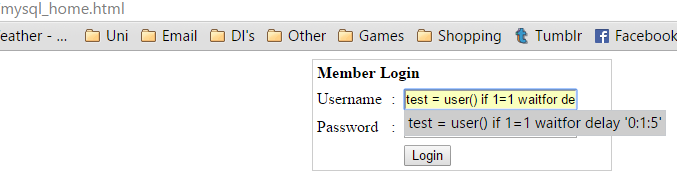




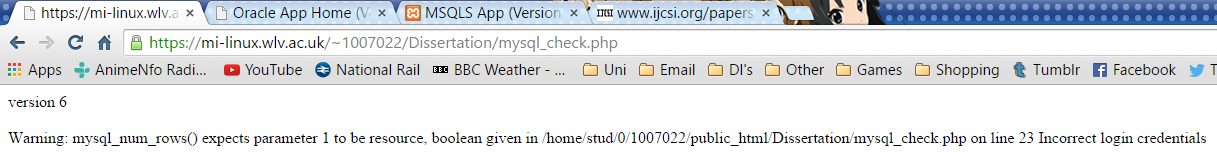
5f) MSQLS Blind Injection attack results



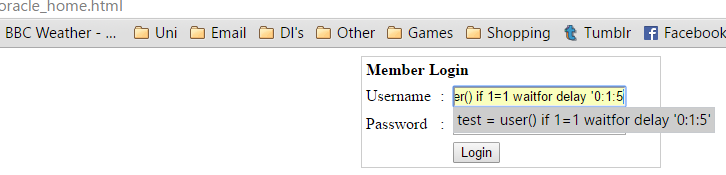
6a) MySQL Timing Attack



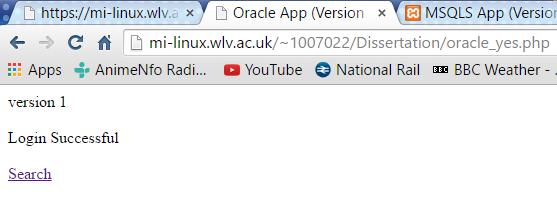
6b) MySQL Timing Attack results



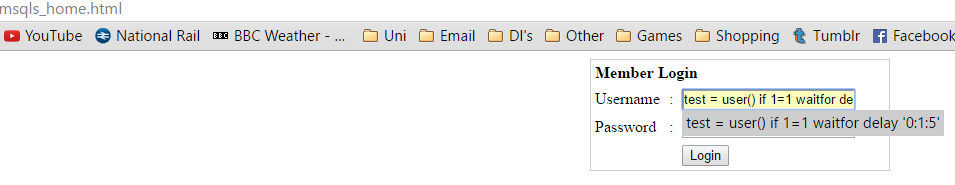
6c) Oracle Timing Attack



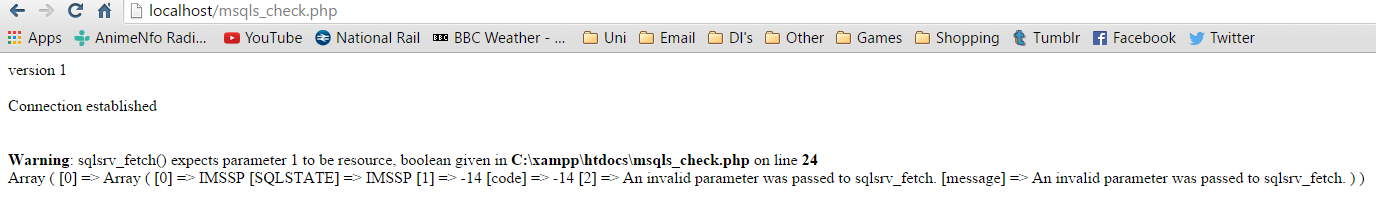
6d) Oracle Timing Attack results



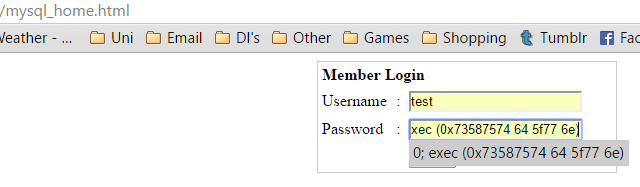
6e) MSQLS Timing Attack



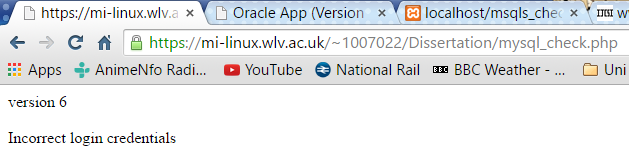
6f) MSQLS Timing Attack results



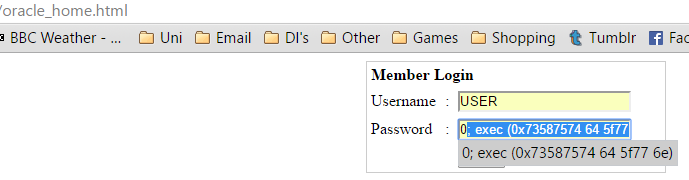
7a) MySQL Alternate Encodings Attack



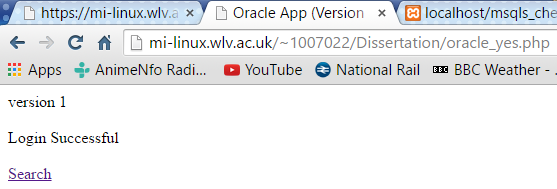
7b) MySQL Alternate Encodings Attack results



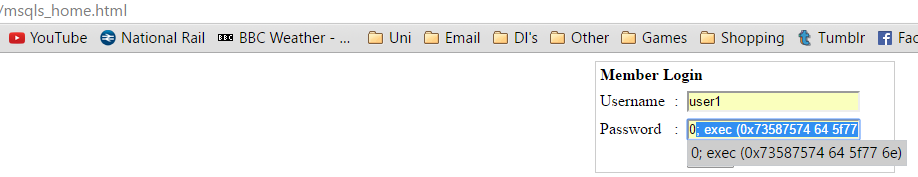
7c) Oracle Alternate Encodings Attack

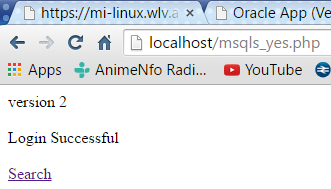


7d) Oracle Alternate Encodings Attack results



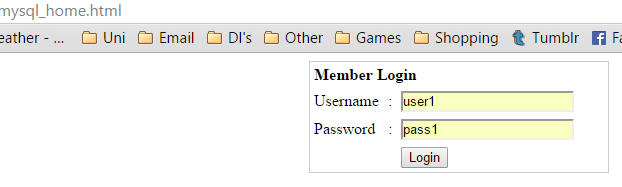
7e) MSQLS Alternate Encodings Attack

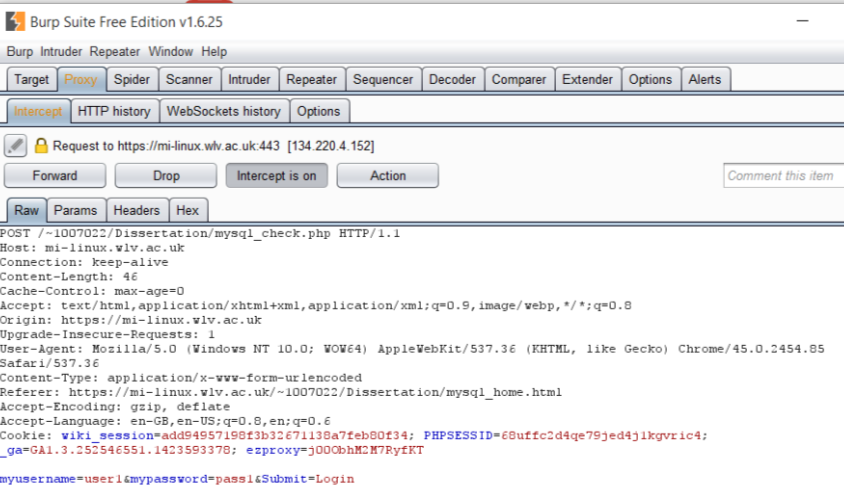


7f) MSQLS Alternate Encodings Attack results

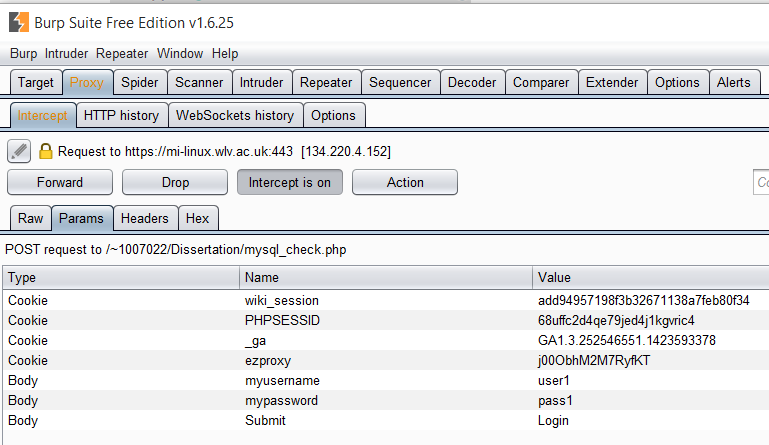
8a) SQLIA results

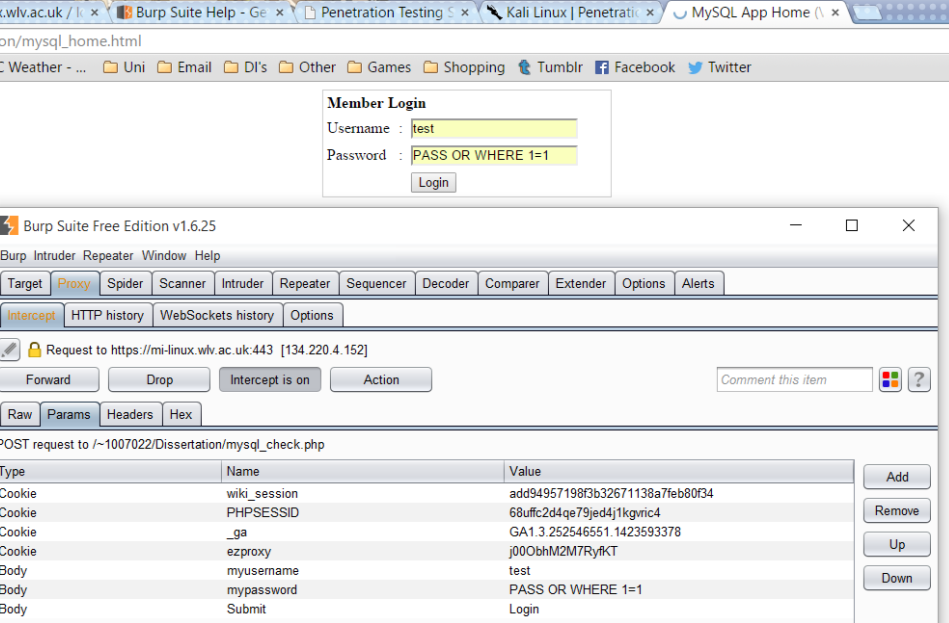
8b) Burp Suite testing

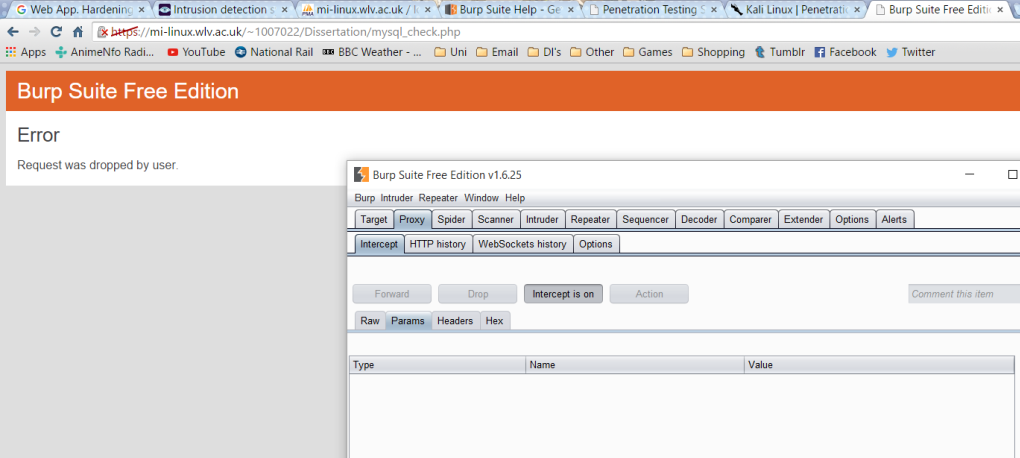


Login request is sent.

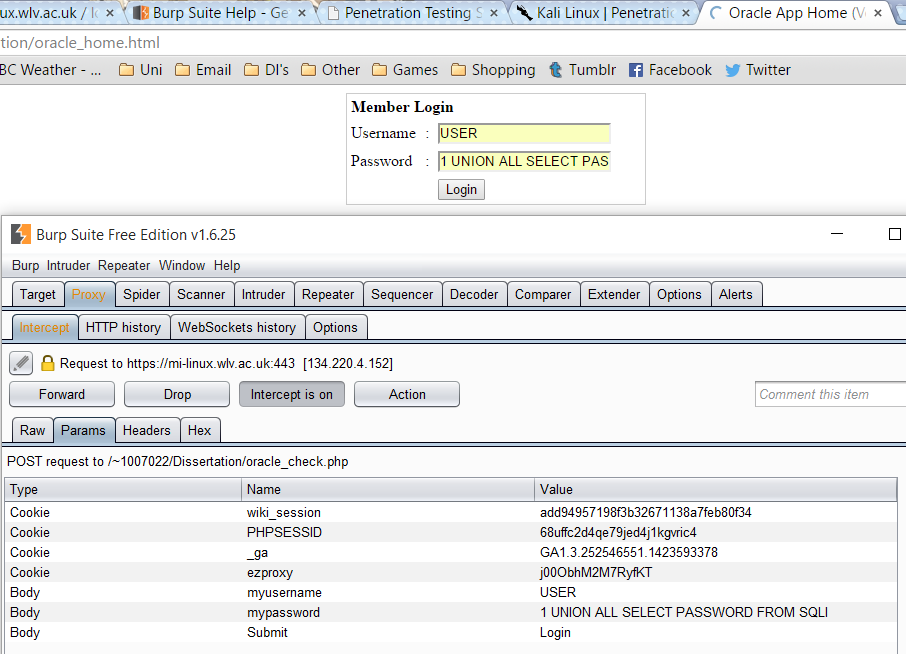
Program detects and outputs details of the request before it can be sent.

Program goes further to show user input.

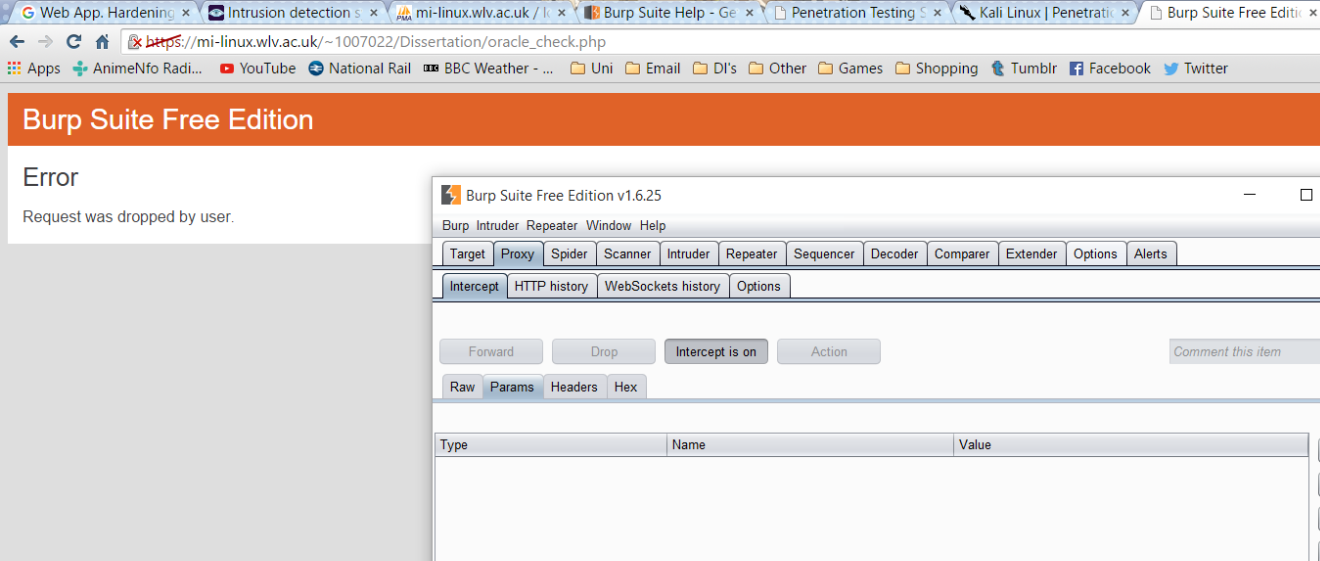
Program detects another request, this time a SQL Injection attempt which is intercepted and its contents shown in order to determine whether it is hostile in nature.

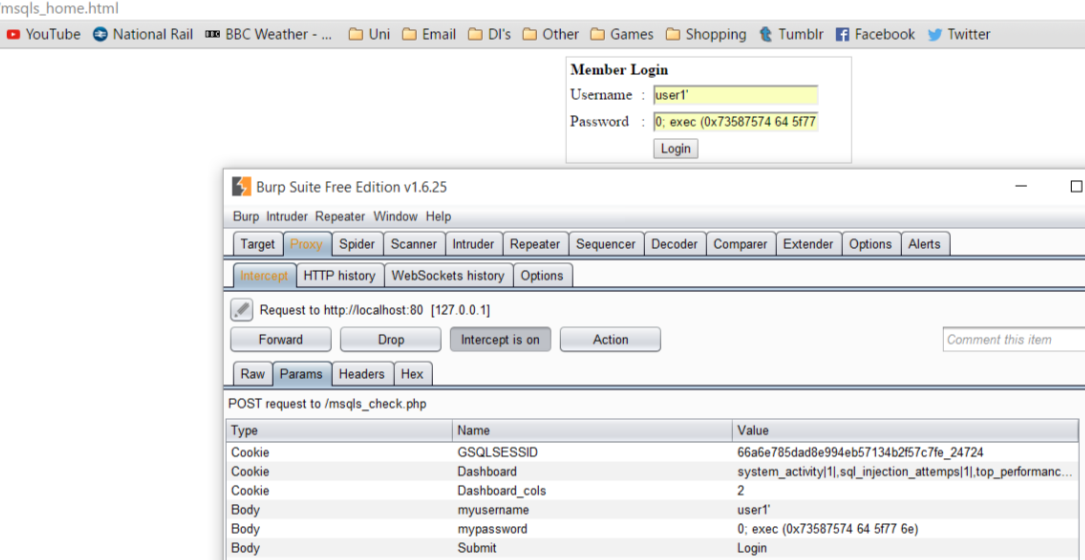


Program can then block the request by dropping it effectively detecting and preventing SQL injection.

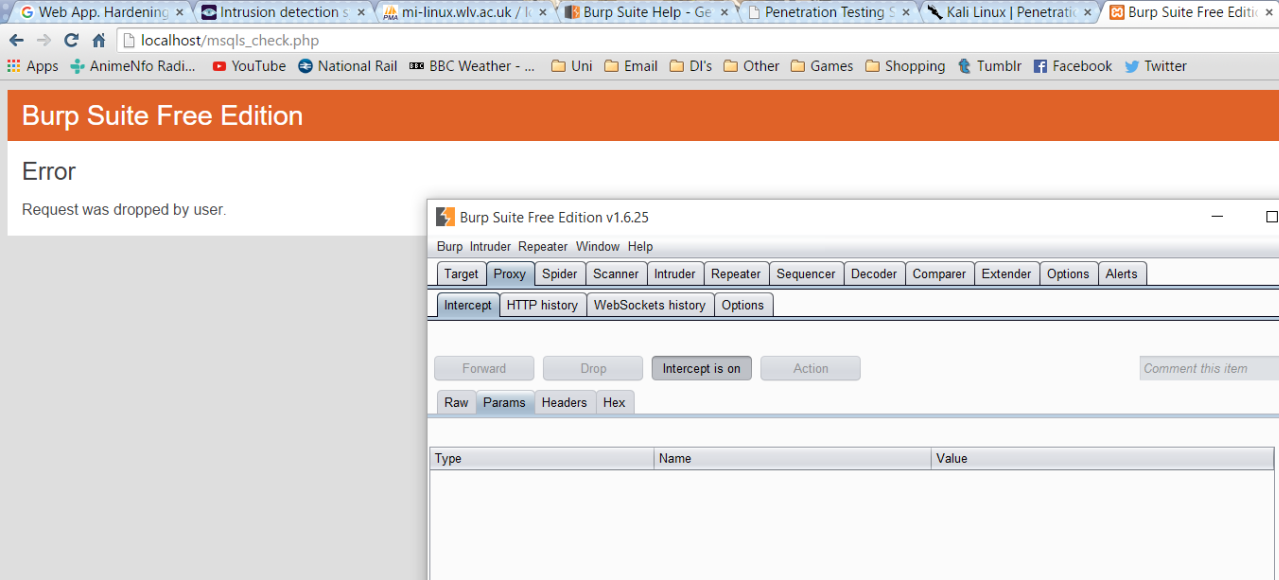


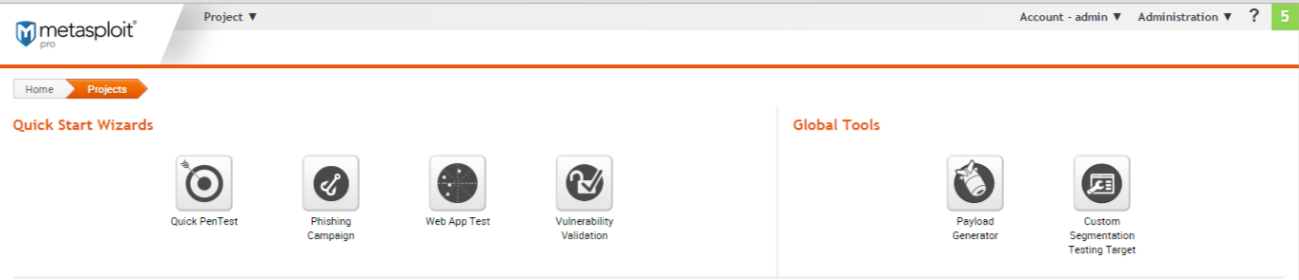
Oracle test

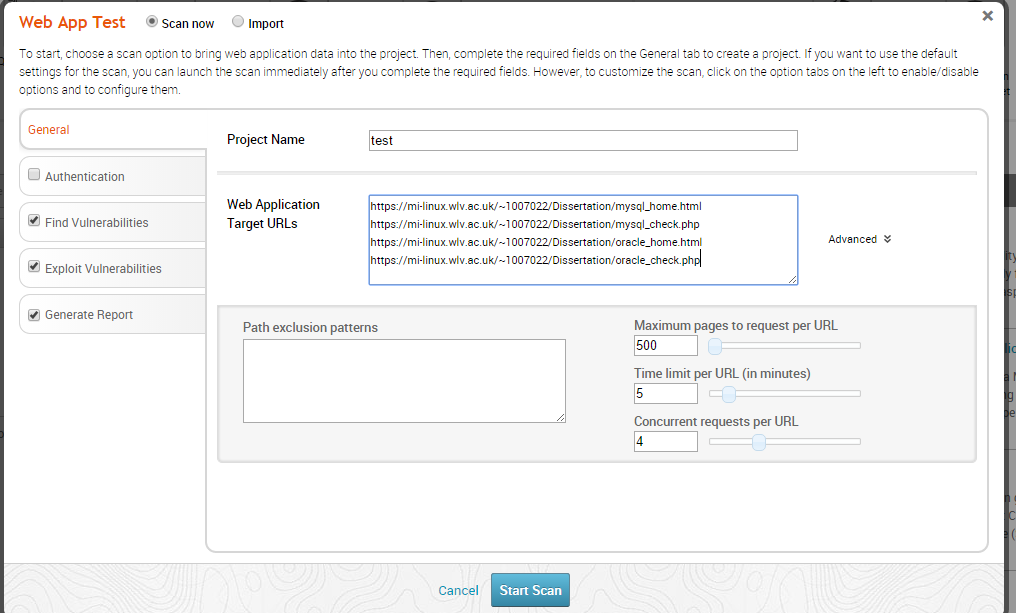




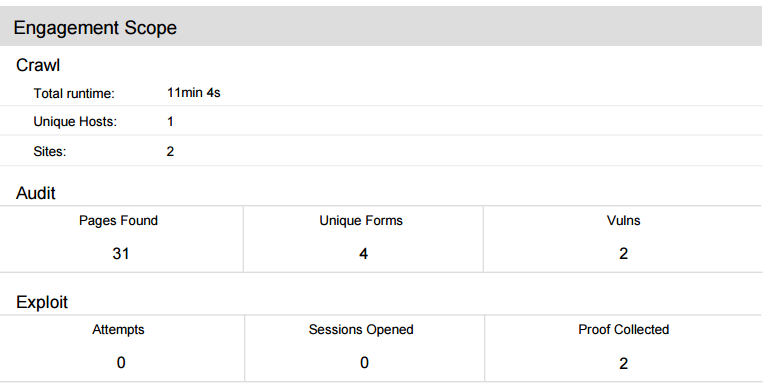
MSQLS test



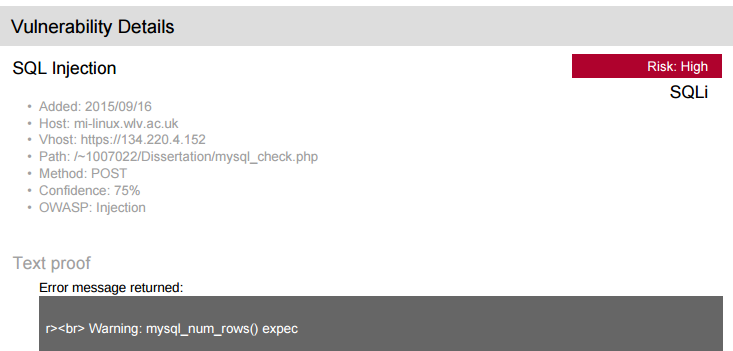
8c) Metasploit testing

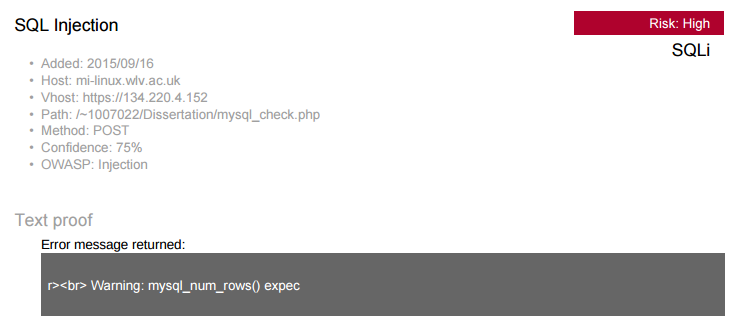
The program allows for testing of a web applications security with several tools such as a penetration test, sending dubious emails, a full application test, vulnerability scanner and more.

The application test was configured to locate the targets, find and exploit and vulnerabilities they have, the results of which will generate a report.



The program found two vulnerabilities.





Both vulnerabilities are shown in detail to be SQLI vulnerabilities and provides advice on dealing with them, which outlines the programs usefulness in combating SQLIAs.