**BWAPP exercise**

1. A1 - Injections

a) OS Command Injection Probably there is something bad happening on server side, try to extract all linux users (hint: passwd).

Please describe your solution here…

b) PHP code injection Try to print some text and then ﬁnd a way to display server critical information (phpinfo).

Please describe your solution here…

2. A2 - Broken Authentication

a) There is a captcha box popping up, try to avoid it using proxy tool

Please describe your solution here…

3. A5 - Security Misconﬁguration

a) Cross Origin Recourse Sharing (AJAX). Create a small website with script that makes request to our vulnerable web application (http://192.168.30.135/bWAPP/sm cors.php) and receives some information from the server (hint: XMLHTTPRequest function).

Please describe your solution here…

4. A7 - Missing Functional Level Access Control

a) Directory Traversal - Directories List some directories which are on the server by changing url.

Please describe your solution here…

b) Directory Traversal - Files Now try to extract some ﬁle’s content.

Please describe your solution here…

c) Host Header Attack - Cache Poisoning Change destination host.

Please describe your solution here…

d) Restrict Device Access You are using computer and the website requires mobile device when using it. Try to achieve this by hacking request.

Please describe your solution here…

e) XML Entity Attacks Inject XML script to display password ﬁle.

Please describe your solution here…

5. A9 - Using Known Vulnerable Components.

a) PHP CGI Remote Code Execution Again edit request and inject php script.

Please describe your solution here…