**Google Gruyere**

1. Perform some scanning using tool called Nikto and Vega. Is the application vulnerable to bad id requests?

Please describe your solution here...

2. Some client state manipulations

a) Intercept some cookie and headers when creating user account (Burpsuite or WebScarab can be useful).

Please describe your solution here...

b) When intercepting parameters during registration try to become admin of this webiste (hint: maybe ﬁeld is author can be replaced with something else).

Please describe your solution here...

c) It seems there are some server generated tokens, try to explain how to modify cookie and get desired privileges.

Please describe your solution here...

d) Maybe there is some way to directly manipulate (token).

Please describe your solution here...

3. XSS - injecting code and cookie stealing

a) Reﬂected

i) Find some input ﬁelds where You can perform XSS (snippets).

Please describe your solution here...

ii) Try at least 5 diﬀerent ways of doing the prevous step (this website may be helpful: https://www.owasp.org/index.php/XSS Filter Evasion Cheat Sheet).

Please describe your solution here...

b) Stored

i) It seems visitors can see some of users proﬁle information. Probably there is a way by clicking or mousing over, some script is being run.

Please describe your solution here...

ii) Try to inject XSS using HTML attributes to your proﬁle information.

Please describe your solution here...

iii) We also have some ﬁle upload tool, try diﬀerent ﬁle types, are there any restrictions?

Please describe your solution here...

iv) Use ﬁle upload to extract some website information.

Please describe your solution here...

4. CSRF

a) Make research on how the url and requests looks like creating or deleting snippet.

Please describe your solution here...

b) Try to perform CSRF attack that deletes the snippet.

Please describe your solution here...

c) Now it should be easy to change password when user is logged in.

Please describe your solution here...

5. Information disclosure

a) Ty to extract database (hint: have a look at the source ﬁle in Gruyere Web Application and try to display it in the website url).

Please describe your solution here...

b) Now we want to display database so that everybody can see it! Make some research how are python variables used in website ﬁles and inject this code into your snippet (hint: x).

Please describe your solution here...

c) Maybe there is also some other way to ﬁnd information using ﬁle upload?

Please describe your solution here...

6. Overload the server

Now when You know how to access web application conﬁguration ﬁles and variables, let’s try to read really big bunch of data.

Please describe your solution here...