	TDT423	37 Software S	ecurity 20	014
	Vu	Inerability Report	ng Form	
		Exercise 1, part	2	
Tested by:	Group 03			
Date:	24.09.2014			
Vulnerability ID	Source Reference	Attack	Risk	Comments
Group number + _ + 4- digit sequence number (E.g. G01_0001)	Where (URL) and What	OWASP attack ID or create your own and explain attack in comments section	Low, Medium, High (= probability x consequence)	
G03_0016	http://tdt4237.idi.ntnu.no:5003/admin/delete/ <username>/</username>	OTG_AUTHZ_004 [1]	High	G03_0015 in part 1, but failed to identify it as Insecure Direct Object Reference. Anyone can use this link to delete users, without being admin or even logged in. The page reports an error message, but the user is deleted anyway.
G03_0017	User.php, line 155	OTG_AUTHN_007	Low	Username can include underscore, even though the password policy says it only can be letters and numbers.
		Both codes from OWASP Testing Guide v4		

[1] Both codes from OWASP Testing Guide v4

.