TDT4237 Software Security 2014

Vulnerability Reporting Form

Exercise 1, part 1

Tested by:	Group 03
Date:	16.09.2014

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_0001	http://tdt4237.idi.ntnu.no:5003/?msg=<HTML>	OWASP-DV-012	High	The url in source reference can be used to craft a special link to other users which can inject javascript or html code.
G03_0002	http://tdt4237.idi.ntnu.no:5003/	OWASP-DV-005	High	Every input field on the entire site except the password fields can be used for SQL injection. This can be done by starting the input data with a single ' and a special crafted SQL statement.
G03_0003	http://tdt4237.idi.ntnu.no:5003/	OWASP-SM-002	High	By editing the isadmin field in the cookie to yes you will be granted administrator rights on the entire site.
G03_0004	http://tdt4237.idi.ntnu.no:5003/user/edit/	OWASP-DV-002	High	XSS: One can inject html into input fields to load scripts from other resources
G03_0005	http://tdt4237.idi.ntnu.no:5003/user/edit/	OWASP-SM-005	High	CSRF: There is no implemented CSRF-protection, thus in the edit profile input form, and admin forms, a malicous adversary can trick a user into performing actions with side effects from another site.
G03_0006	http://tdt4237.idi.ntnu.no:5003/user/<USERNAME>/	OWASP-IG-003	High	One can inspect the html page source of a user profile to find the users password hash.
G03_0007	http://tdt4237.idi.ntnu.no:5003/user/<USERNAME>/	OWASP-AT-004	High	The password hashes is not salted, and the password may be calculated with ease using bruteforce.
G03_0008	http://tdt4237.idi.ntnu.no:5003/movies/left.jsp	OWASP-IG-006	Medium	Stack trace should not be public. Here is an example of one. In combination with G03_0002 one can prod the database to return details of its internal structure and technology stack (frameworks etc.)
G03_0009	http://tdt4237.idi.ntnu.no:5003/movies/<id>/	OWASP A7	Low	Lacking access control to movie review. In combination with G03_0002, this allows non-authenticated users and robots to spam the site
G03_0010	http://tdt4237.idi.ntnu.no:5003/user/new/	OWASP-AT-003		There is no requirements on different characters or symbols used or the length of the password. The password can be one character and can be easily found.
G03_0011	http://tdt4237.idi.ntnu.no:5003/	OWASP-SM-001	Medium	There is no session timeout on the site.
G03_0012	http://tdt4237.idi.ntnu.no:5003/	OWASP-SM-002	High	Due to the lack of HTTPS, session ID's can be hijacked.
G03_0013	http://tdt4237.idi.ntnu.no:5003/	OWASP-IG	Low	The password field in the login is not a password field, it is a normal textfield. That means that the password is showing, when writing it and passwords typed before are listed when the field is edited (in most browsers).
G03_0014	http://tdt4237.idi.ntnu.no:5003/users/	OWASP-IG	Medium	Information leak: All the usernames are listed on the site, even for not logged in users.
G03_0015	http://tdt4237.idi.ntnu.no:5003/admin/delete/<USERNAME>/	OWASP-CM-007	High	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.