Zap Test Document

Manual test completed, created user zaptest did a story and commented a couple stories.

The automatic test found 2 errors, one in which you can add a comment without indicating to what story, solved, and a second one with adding a comment with no text, also solved in code.

Found a problem with the cascade constraints that doesn’t work to delete a story that has comments, so change the code at the story context level so first searches for each story on the list and erase all of them on the table. That one was cool to solve!

// ---- All that was Before the active test. //

Some how Zap still finding a way of try to save a comment with no story attached.

After running the test, I’ll be focusing on the 3 Cross site Scripting alerts, high risk but Low confidence and they are on the login page.  
and 1 remote OS command injection with Medium confidence.

For that one I found that I had a hidden control input with no validation and no check , which was producing a lot of errors of “ comment not attached to a story, object not set to a value” , I believe I got it adding a check to the DB to see if the story exists before trying to add a comment to it.

And taking a look at this video <https://www.youtube.com/watch?v=K9_JQke0YaA> it looks like my web won’t execute the code, it just gives an error.

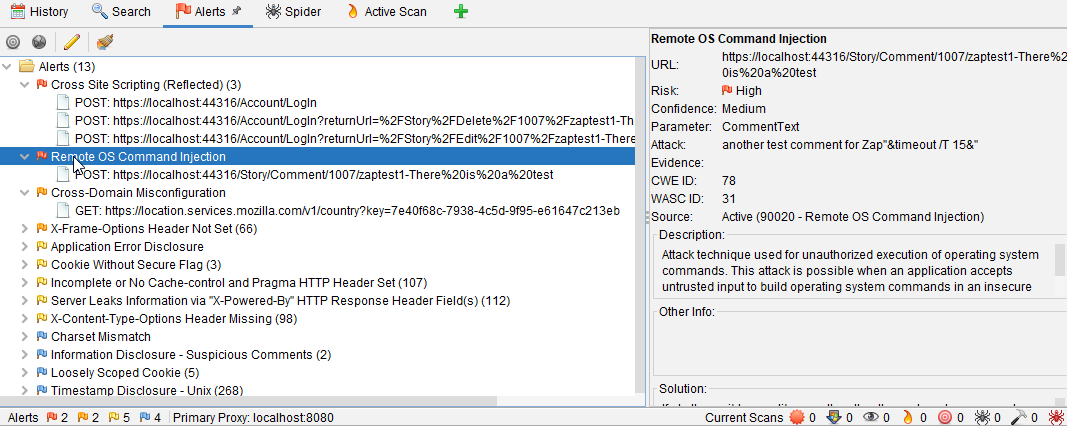
2 Screenshots on the bottom of the document just in case.

The complete list:

* Cross Site Scripting (Reflected) (3)
* Remote OS Command Injection
* Cross-Domain Misconfiguration
* X-Frame-Options Header Not Set (66)
* Application Error Disclosure
* Cookie Without Secure Flag (3)
* Incomplete or No Cache-control and Pragma HTTP Header Set (107)
* Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (112)
* X-Content-Type-Options Header Missing (98)
* Charset Mismatch
* Information Disclosure - Suspicious Comments (2)
* Loosely Scoped Cookie (5)
* Timestamp Disclosure - Unix (268)

And after fixing some stuff :

* Cross Site Scripting (Reflected) (2)
* POST: https://localhost:44316/Account/LogIn
* POST: https://localhost:44316/Account/LogIn?returnUrl=%2FStory%2FEdit%2F2065
* Application Error Disclosure
* Cookie Without Secure Flag
* Incomplete or No Cache-control and Pragma HTTP Header Set (4379)
* Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (6606)
* Information Disclosure - Suspicious Comments (2)
* Loosely Scoped Cookie



* Timestamp Disclosure - Unix 