**TECHKNIGHT’S FIRST VULNERABILLITY ASSESSMENT**

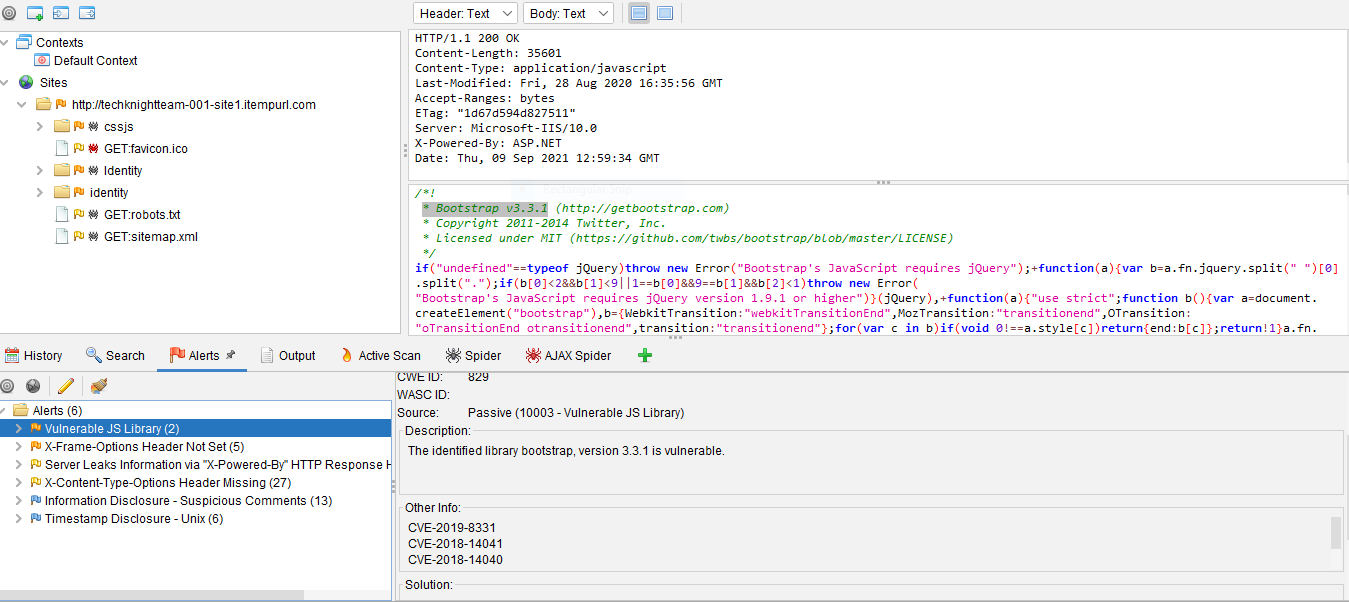
**DATE: 9th September,2021**

From the vulnerability scan there are:

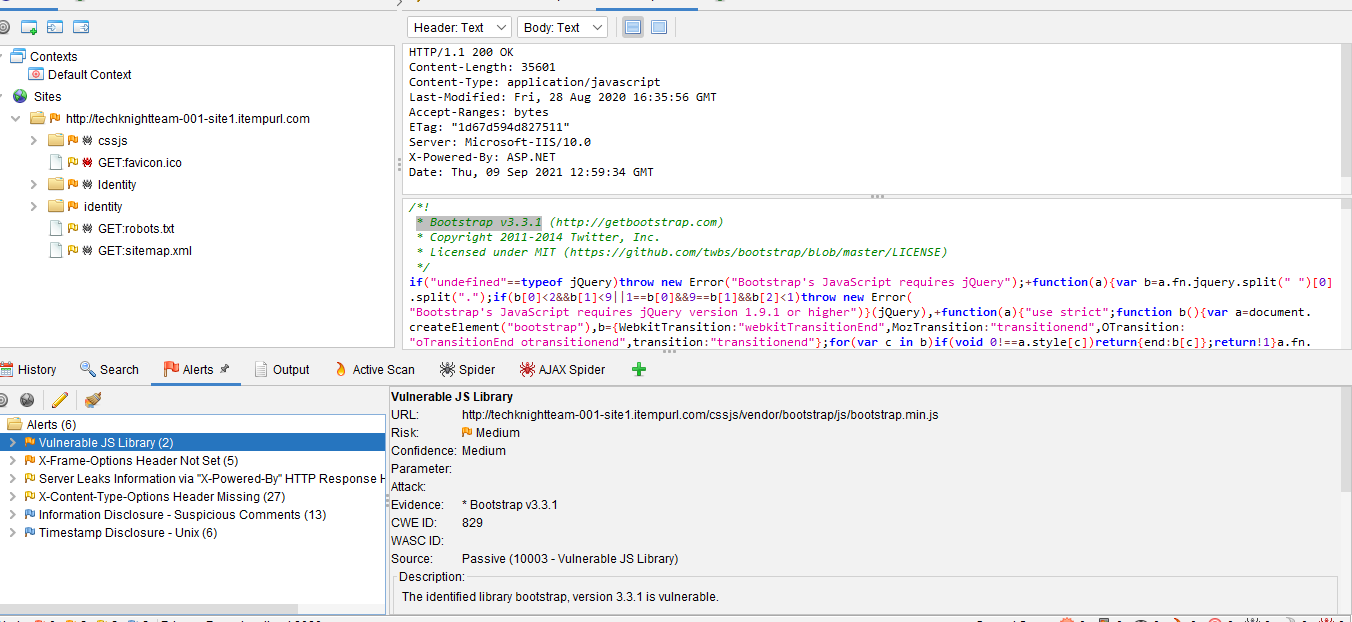
2 medium risk alerts,

2 low risk alerts

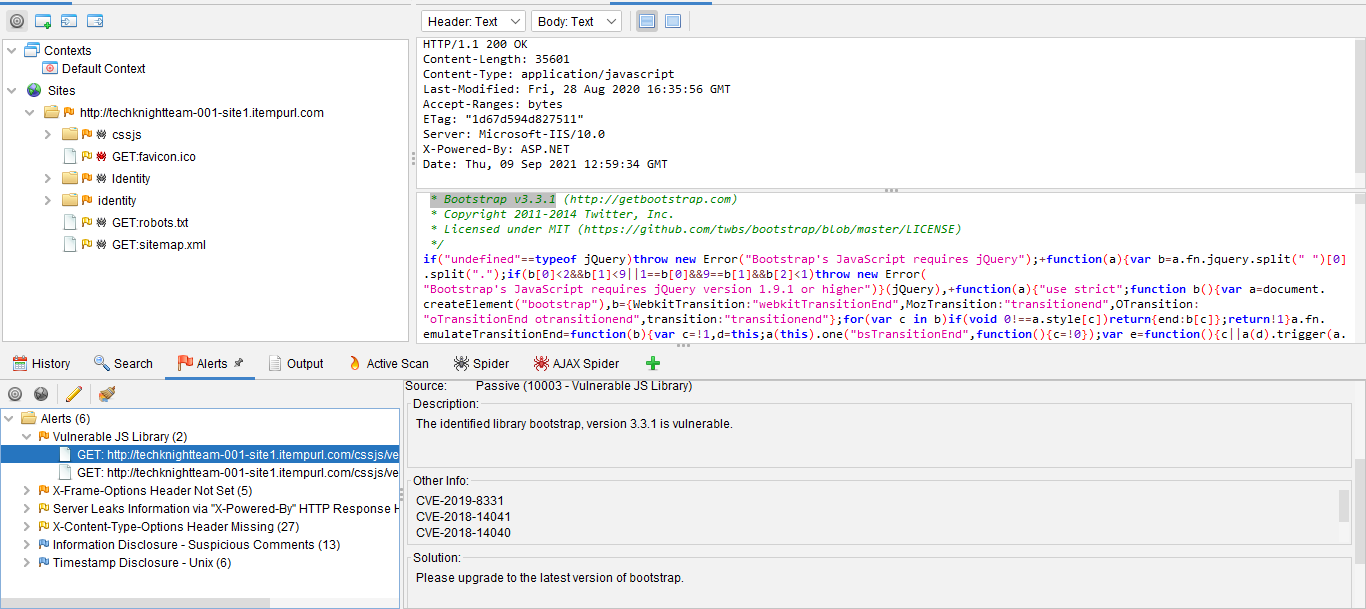
2 informational alerts



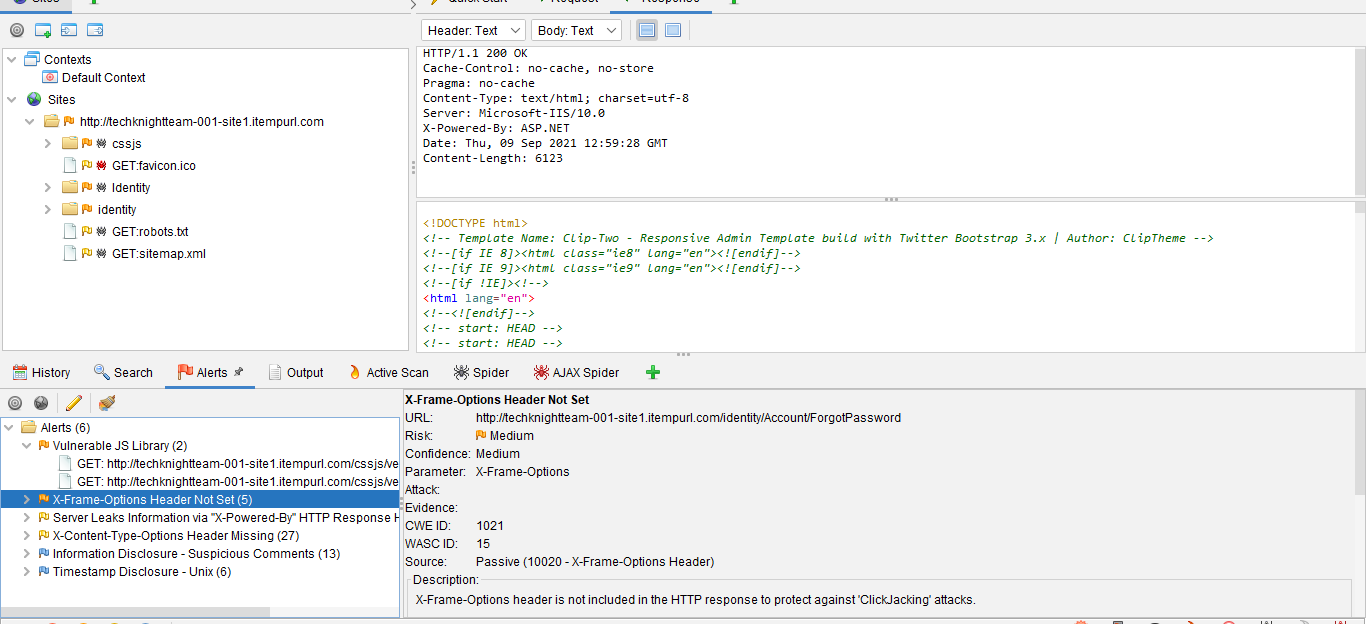
1a Vulnerable JS library (medium risk)



1b. Solution is to upgrade to the latest version of bootstrap

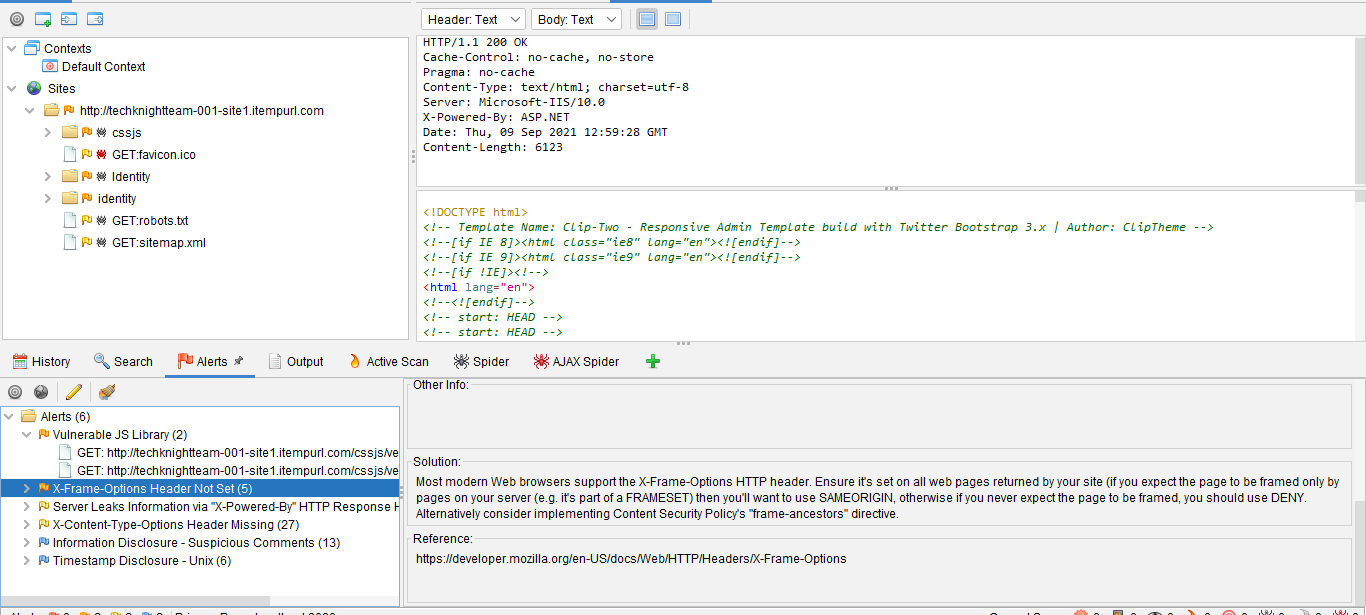


2a. Xframe headers not set (medium risk)

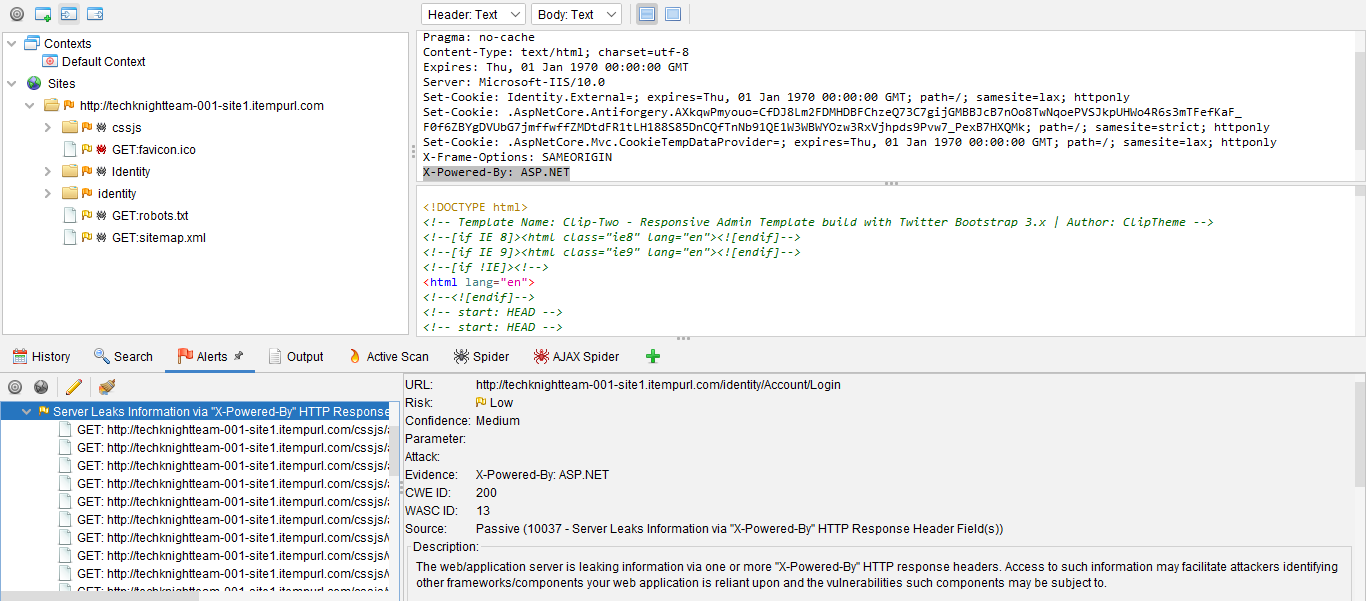


2b. Solution;

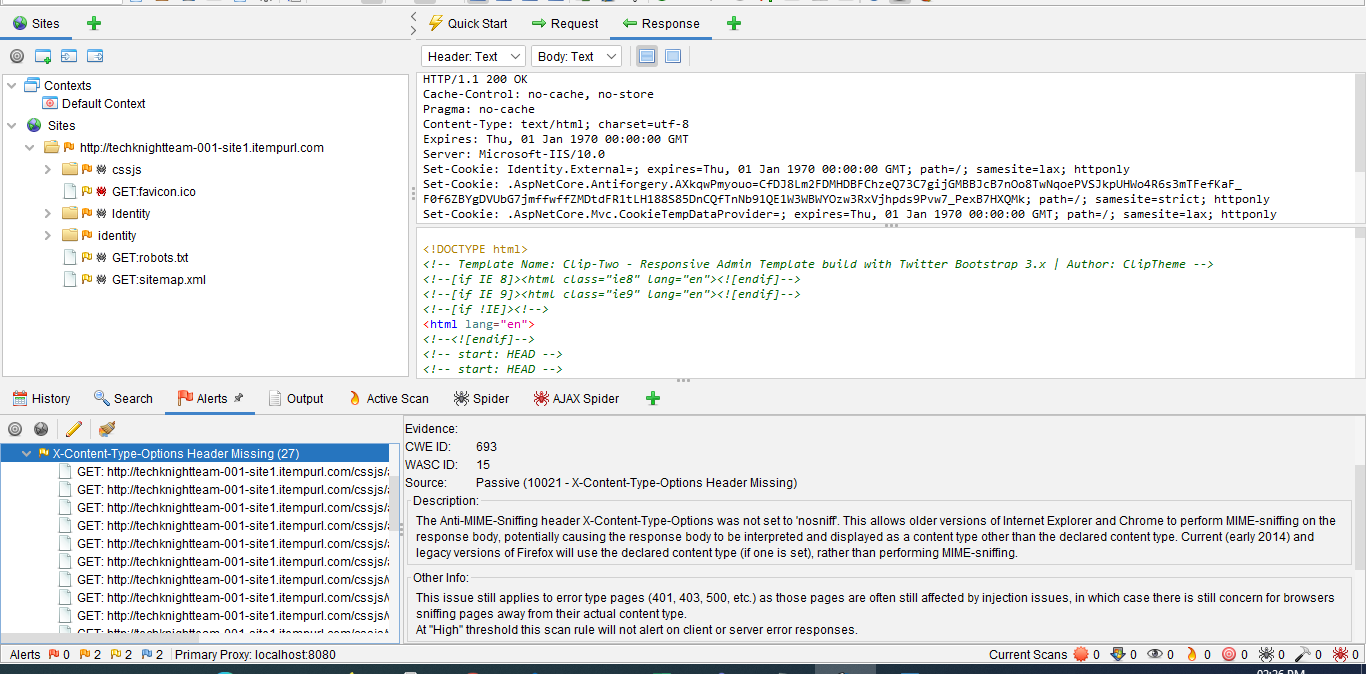
Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive

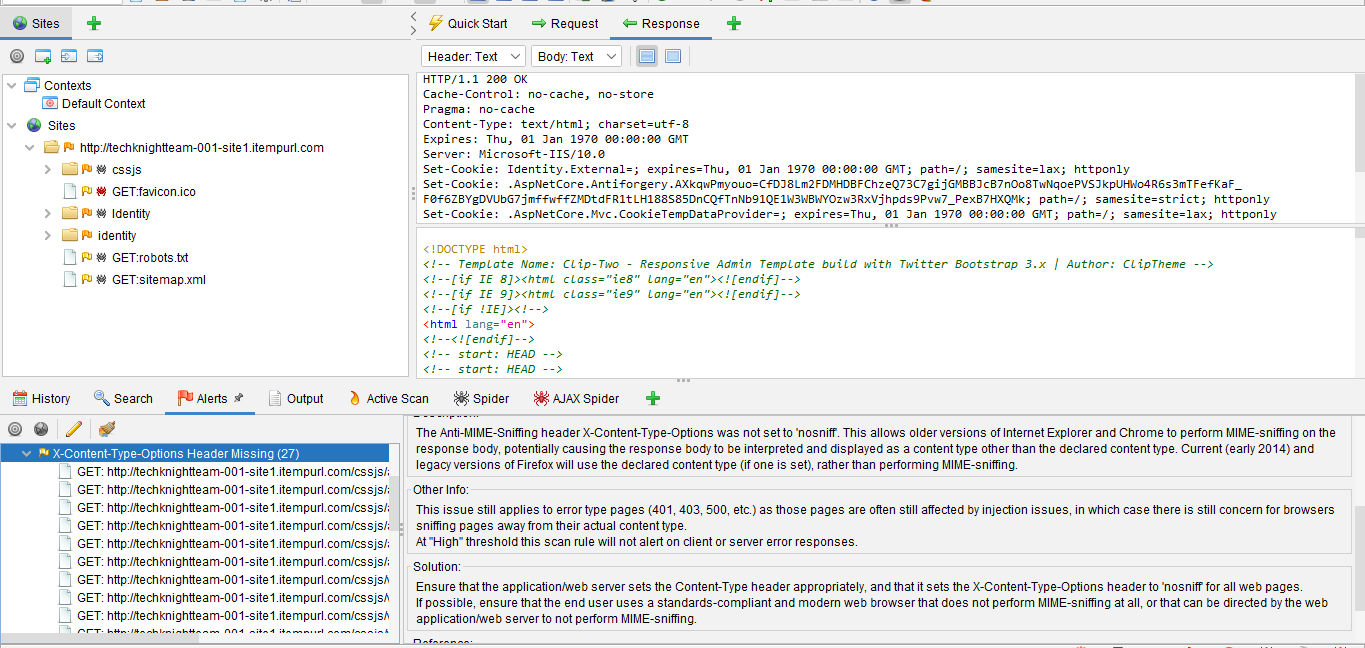


3a. Server leaks Information (low) the leak is highlighted in the top right section

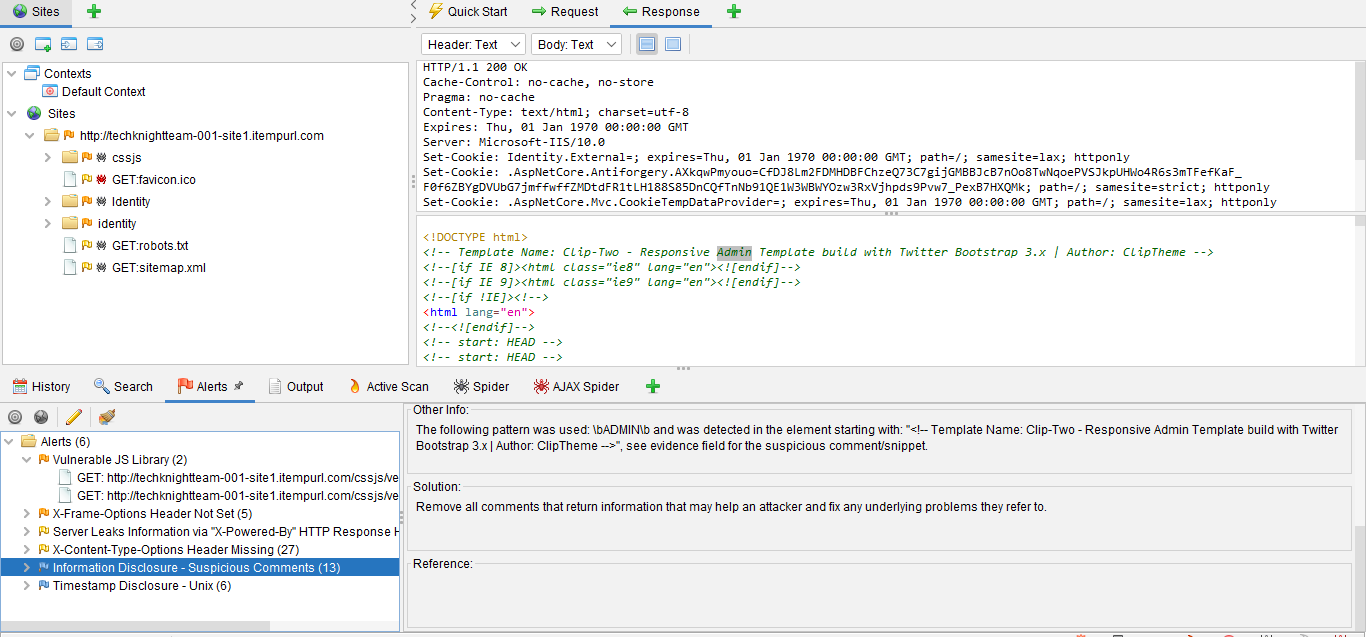


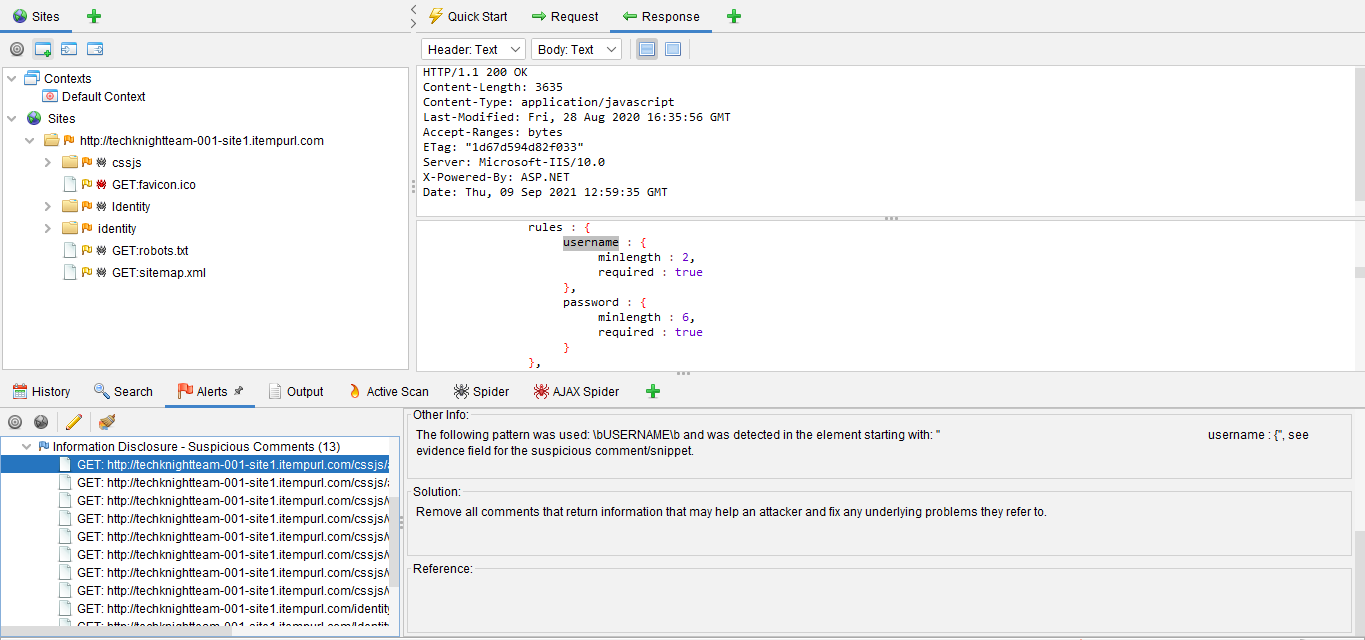
3b. Solution X content type was not set to no sniff please ensure content type is set correctly set X-content type to no sniff on all web pages.





4a.Information disclosure ( informational alert) contains information that might help an attacker)





4b.Timestamp disclosure (informational alert)

