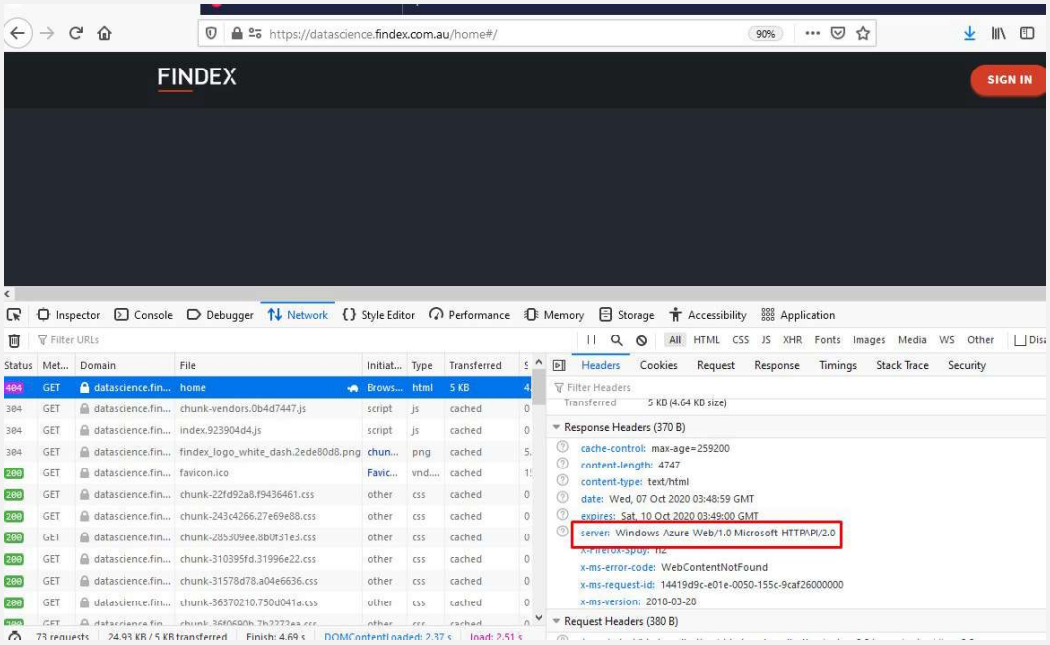


II	Server Banner Disclosure
Description	We identified that the application's response header leaks the server software being used. This identified information can be used by the attacker to limit their attack vectors to identified server software letting them attack in less time frame than usual.
OWASP Top Ten 2017	-
Affected URL/IP	https://datascience.findex.com.au/home#/
Steps to Reproduce	<p>1. Goto https://datascience.findex.com.au/home#/</p> <p>2. Open developer tools in the browser, then goto Network Tab and press "Reload"</p> <p>3. Click on the first request to the above URL and check the response header.</p> <p>4. You can see something similar to the below screenshot leaking server banner in the Server Header:</p> 
Remediation	From the configuration, edit the server.xml file to remove the server banner data.
References	<ul style="list-style-type: none"> https://owasp.org/www-project-web-security-testing-guide/latest/4-W eb_Application_Security_Testing/01-Information_Gathering/02-Finger print_Web_Server https://www.ibm.com/developerworks/library/se-banner/index.html