The preceding request and response demonstrate how ZAP captures the interaction that led to the alert. In the SQL injection example ZAP injected a payload

into the txtpwd parameter and observed server behavior consistent with unsanitized input being executed on the backend. This level of evidence is valuable
because it enables reproduction and remediation by developers. Note also that
ZAP did not discover any issues that require authenticated access during the
unauthenticated scan.
13.3 Authenticated Scans Using ZAP
Authenticated scanning broadens the test surface by including pages and features
that are visible only after login. To perform an authenticated scan with ZAP use
the Manual Explore option, provide the application URL, enable the Heads Up
Display (HUD), and launch the browser through ZAP. The browser that ZAP
launches may display a security warning due to ZAP ’ s interception certificate.
Proceed to the application and authenticate with an account that has relevant
privileges, for example an administrative user. This allows ZAP to record traffic
while exercising authenticated workflows.
... (content truncated for brevity in this code block)