SCENARIO

The application contains a reflected cross site scripting vulnerability in the search box functionality because it backslashes any unexpected character including single quotes automatically in order to prevent user from breaking user out of the attribute. We will try to trigger an alert message by injecting a payload into the application.

**PROCEDURE**

1. Go to the vulnerable application and search for anything containing a single quote and we see that it got back slashed.
2. In this scenario we will try to break out of the parent </script> tag in order to execute any malicious script.
3. At the end, we will create a payload depending on the conditions of the application so that we can generate an alert to exploit the vulnerability.

**PAYLOAD**

</script><script>alert("HACKED!")</script>

**REMEDIATION**