Task 4:

A description of the attack you performed to successfully login as admin. Include the attack string (correctly encoded) you used to do the attack.

The attack exploited improper validation of the url parameter during login. By injecting the encoded payload %2Fsecure%2F%0ASet%2DCookie%3A%20MOD%5FBUT%5FUsername%3Dadmin into the url parameter, the WAF was tricked into setting a Set-Cookie header that granted admin access. This is a form of HTTP Request Smuggling, bypassing the WAF's authentication mechanism.

The response (the displayed webpage) of the web application you received after a successful login as admin.