**(A2) Broken Authentication - Password Reset**

# **BACKGROUND**A red padlock with the illustration of a goat is unlocked.

While most websites use some form of authentication, it is quite common for authentication to be "broken". In other words, there may be other ways to authenticate besides the original intended method.

# **DESCRIPTION**

This exercise will explore a few common "broken" authentication mechanisms.

# **REQUIREMENTS**

A computer that can run Java. Most modern Windows, Linux and MacOS machines can run Java, as can Google Cloud Shell. This exercise assumes you’re running an instance of Linux (either virtualized or other). This exercise will run in Google Cloud Shell. Previous exercises in this chapter walk through the Java and WebGoat installations. A web browser (preferably Chrome) is also required.

# **PART I: Password reset (Steps 1, 3 and 4)**

1. Log into WebGoat
2. From the left navigation bar, select "(A2) Broken Authentication"
3. From the left navigation bar, select "Password reset"
4. Click on Step 1 (a gray box) and learn about password reset vulnerabilities
5. Click on Step 3 (a gray box) and learn about a method to find out if an account exists
6. Click on Step 4 and try to recover a password. HINT: The instructions provide some account names to try

# **PART 2: Password reset (Steps 5 and 7)**

1. From the left navigation bar, select "(A2) Broken Authentication"
2. From the left navigation bar, select "Password reset"
3. Click on Step 5 (a gray box) and complete the assignment
4. Click on Step 7 and learn about some mitigation tactics

| EVIDENCE #1 |
| --- |
| **PASTE THE IMAGE OF THE LESSON ("PASSWORD RESET") AND STEPS 4 AND 5 AS GREEN** |