# AdvWAF Lesson 1 – Application Security Overview

Exercise – Examine OWASP Attacks

* Required virtual images: BIGIPA and Win Jumphost
* Estimated completion time: 15 minutes

### Task 1 – Verify Web Site Vulnerabilities

Access the DVWA web application and attempt two well-known attacks against the application.

* On the UDF **Deployments** page, for the **WWFE – AdvWAF v15.1** blueprint open the **Components** page.

**→NOTE:** This assumes you’ve already started your deployment this morning.

* In the **Systems** section for **Windows Jumpbox** select the **Access** list and click **RDP** to access the Windows desktop, and then log in
* Open **PuTTY** and open the BIGIP\_A
* At the CLI copy and paste the following TMSH commands. (NOTE: Use the “WWFE-AdvWAF v15\_1 copy and paste guide” inside the **Windows Jumpbox Documents** directory.)

tmsh create ltm pool dvwa\_pool members add { 10.1.20.17:80 { address 10.1.20.17 } }

tmsh create ltm virtual dvwa\_virtual destination 10.1.10.35:80 ip-protocol tcp profiles add { tcp { } http { } } security-log-profiles add { "Log all requests" } pool dvwa\_pool

exit

* Open a new Firefox window and click the **DVWA** bookmark, and then log in

SQL Injection

* On the navigation menu click **SQL Injection**, then type **6** in the **User ID** field, and then click **Submit**.

The purpose of this feature is to print the ID, first name, and surname of the submitted user ID. This is the expected behavior of this feature.

* Copy and paste the following in the **User ID** field, and then click **Submit.** (NOTE: Use the copy and paste guide inside the **Documents** directory.)

1111

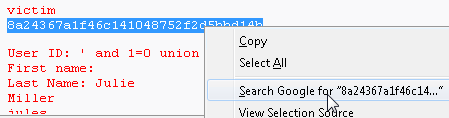
You are presented with all the users in the database.

* Copy and paste the following in the **User ID** field, and then click **Submit**.

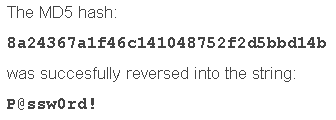
2222

This statement returns the user ID, first name, last name, user name, and password (in a hash format) of all users in the **users** table.

* Note that there is a user named **Victim User** with the username of “**victim**”.
* Select the hashed password value for **victim**, and then right-click and select **Search Google for “8a24367a1f4…”**.



* Select the first link with the decoded hash value and note the decoded password value.



The decoded value is “**P@ssw0rd!**”.

* Close the tab, then on the DVWA page click **Logout**, and then log back in as **victim** / **P@ssw0rd!**

At the bottom of the page note that we’ve successfully logged in with another user’s credentials.   
A successful SQL injection exploit can read sensitive data from the application database, modify database data, or even delete data or the entire database.

