[Date]

Lalit Mangale

**WebGoat Installation and Completion Report on Windows**

Cybersecurity Training / VAPT Practice

Web-Goat Installation and Completion Report on Windows

# Objective

The objective of this report is to document the installation and usage of WebGoat on a Windows machine for learning and practicing web security vulnerabilities.

# Installation Steps on Windows

## Step 1: Install Java

* WebGoat requires Java 8 or later.
* Download Java from [https://adoptium.net/](https://adoptium.net/%20) or <https://www.oracle.com/java/technologies/javase-downloads.html>.
* Install Java and verify installation by running:

java -version

|  |
| --- |
| **Java Version Check JDK-24** |

## Step 2: Download WebGoat

* Visit <https://github.com/WebGoat/WebGoat/releases.>
* Download the latest .jar file (e.g., webgoat 2025.3.jar).

|  |
| --- |
|  |
| **Click on webgoat-2025.3.jar** |

## Step 3: Run WebGoat

* Open **Command Prompt (cmd)**.
* Navigate to the download location:

cd Downloads

* Run WebGoat:

java -jar webgoat 2025.3.jar

|  |
| --- |
|  |
| **Open with java -jar** |

* WebGoat should be accessible at[: http://localhost:8080/WebGoat](:%20http:/localhost:8080/WebGoat)

|  |
| --- |
| **Webgoat Login** |

# Using WebGoat

## Login

* Open a browser and go to <http://localhost:8080/WebGoat>.
* Create a new user account.

|  |
| --- |
|  |
| **Register as New User** |

* Login with the newly created account.

## Practice Exercises

### General:

**Http Basic:** Enter your name in the input field below and press "Go!" to submit. The server will accept the request, reverse the input, and display it back to the user, illustrating the basics of managing an HTTP request.

|  |  |
| --- | --- |
| **1.1 HTTP Request** | **1.2 Request and Magic Number** |

In 1.1 you just type your name in empty column; in result you will see a reverse input on your screen.

In 1.2 you can type request method and any random number in blank space than inspect that page search that inspect that page – go to network – in response section you get a Magic Number.

**HTTP Proxies:** We need Burp Suite or ZAP Proxy (we use Burp Suite)

* Change the Method to GET
* Add a header 'x-request-intercepted:true' (add nywhere)
* Remove the request body and instead send 'changeMe' as a query string parameter and set the value to 'Requests are tampered easily' (without the single quotes)
* Then hit the forward button.

|  |
| --- |
| **Intercept Traffic Via Burp Suite** |

**Developer Tool:**

1. Open inspect section.
2. Go to console section.
3. Type webgoat.customjs.phoneHome()
4. You will get a unique number then pest it.

|  |  |
| --- | --- |
| **Generate a Unique Number** | **Get a result** |

Find a specific HTTP request and read a randomized number.

|  |
| --- |
| **Find Unique number in Inspect section** |

**CIA Triad:**

You must answer 4 MCQ which is based on CIA Triad module.

**Writing New Lesson:**

|  |  |
| --- | --- |
| **Copy that highlighted Parameter** | **Fill that 2 columns with same Parameter** |

## A1) Broken Access Control:

### Hijack Session:

We use Burp Suite for intercept the traffic.

Steep:

1. Go to Burp Suite and open Browser and login.
2. You will get a cookie in inspect element or in Burp Suite Proxy Tab Note it.
3. Log Off that session and Login Again (to see the Cookie value)
4. You can be able to see the last 2-3 digit change every time, so we can do Brute force attack method.
5. Add those last 2-3 Digit and use cluster bombing Method for Brute Force attack.
6. Lastly you will get attack result.

**Note: Sometime cookie will not change immediately so you must clear cache file from your Default Browser.**

|  |  |
| --- | --- |
| **(2)**    **1.1 Cookie Value** | **1.2 Cookie value in Burp Send to Intruder Brute Force Attack** |
| **1.3 After getting numerical sequence add those changing number** | **1.4 After attacking you will get a successful result** |

### Insecure Design Object Reference:

|  |
| --- |
| **(2)**    **Type Given User and Password in empty Box** |

We need Burp suite for next task:

Steep:

1. Open Burp Suite intercept the webgoat traffic.
2. Then click on View Profile, capture that traffic and send this to repeater.
3. Request send to response tab.
4. Your Final Answer: role,userId

|  |  |
| --- | --- |
| **(3)**    **2.1 Intercept traffic via Burp Suite** | **2.2 Sent traffic to Repeater Tab** |
|  |
| **2.3 Your Final Answer** |

Take a reference from image 2.2, it helps to get your answer.

Your last answer: WebGoat/IDOR/profile/2342384

|  |
| --- |
| **(4)**    **Your Final Answer** |

For next task we need another person profile

We need a python script:

|  |  |
| --- | --- |
| **(5)**    **Python Script** | **Replace number with highlighted text** |
| **Replaced With number and forward** | **Final Result** |

Note: for better understand please click here ([YouTube Tutorial](https://youtu.be/qjQ9aW9BhVI?si=wsAbMWP275fBQ8_s))

### Missing Function Level Access control

Steep:

1. Right click and open inspect.
2. Go to network and find MissingFunctionACHiddenMenu than click on it.
3. Go to response and scroll down.
4. Final Answer: Users -- Config

|  |  |
| --- | --- |
| **Response Tab** | **Your Answer** |

## A2) Cryptographic Failure

### Crypto Basic

**Base 64 Decoding: Online Method**

1. Go to google and search “base64decoder” Link: ([Website](https://www.base64decode.org/))
2. Select Decoder and paste the value.
3. After some time, you will get your result.

|  |  |  |
| --- | --- | --- |
| **(2)**    **Copy the given Value** | **Paste it** | **Result** |

**Base 64 Decoding: Burp Suite Method**

1. Open Burp Suite and go to Decoder Tab
2. Then select Decode as Base64

|  |
| --- |
| **(2)** |
| **Final Burp Suite Result** |

**Other Encoding :**

1. We must extract password from XOR Encoding
2. So, we use one website ([Link](https://strelitzia.net/wasXORdecoder/wasXORdecoder.html))
3. **Note**: Please click on LINK and you will get a website
4. Paste the XOR value in first box and click on Decode.
5. Then you will get a result in plain text
6. Your Answer: databasepassword

|  |  |
| --- | --- |
| **(3)**    **Paste value and click on decode** | **Result** |

**Plain Hashing:**

1. Go to Google and search “Hash Cracker” ([Link](https://crackstation.net/))
2. Paste a hash value and hit crack hash.
3. You will get a result in plain Text.
4. Your Answer’s: passwords -- admin

|  |  |  |
| --- | --- | --- |
| **(4)**    **MD5 to Plain Text** | **SHA256 to Plain Text** | **Result** |

**Private to Public Key using OpenSSL with Kali Linux:**

1. Copy all Private key and open Kali Linux and save in note pad, then save that file with .key
2. Open terminal and type openssl rsa -in PVT.key -pubout > Public.pub command for convert PVT key Into Public key.
3. Read that public key we use cat public.pub command.
4. Then we must extract modulus from public key, so we use openssl rsa -in public.pub -pubin -modulus -noout command.
5. Paste modules and now we want to define signature to complete the task.
6. For defining signature we have to eco that Modulus so we use echo -n “” | openssl dgst -sign PVT.key -sha256 -out sign.sha256 command and always put modulus put in Double Quote
7. We now got a sign.sha256 file and we must convert this to base 64 for read that, so we type openssl enc -base64 -in sign.sha256 -out sign.sha256.sha256 command.
8. Then you will get a result

|  |  |  |
| --- | --- | --- |
| **(6)**    **Create text file in Linux** | **PVT Key to Public Key** | **See public key** |
| **Extract Modulus from Public Key** | **Extract the Signature** | **File convert sha256 to base64** |

|  |
| --- |
| **Assignment Done** |

**Challenges Faced**

* Initial difficulty installing the correct Java version.
* Windows Firewall blocking port 8080; fixed by allowing Java through the firewall.
* Some advanced exercises like Blind SQL Injection were complex but manageable with research.

**Completion Proof**

List of completed modules:

* SQL Injection: Completed
* XSS: Completed
* Authentication Bypass: Completed
* *(Insert screenshots showing "Lesson Completed" screens.)*

**Conclusion**

Using WebGoat on Windows provided valuable hands-on experience with web security vulnerabilities. It deepened my understanding of attacks such as SQL Injection, XSS, and Broken Access Control. Practical exercises like these are essential for building cybersecurity skills and knowledge.