Lab-1 Report

Akhilesh Gowda Mandya Ramesh

***Abstract*—The Lab-1 introduces us to the attacks in real world with hands-on experience to stop these attacks during the development process.**

I. Introduction

THIS introduces WebGoat, which is a deliberately insecure web application used to practice security related work and WebWolf which gives a clear picture of the scenario behind an attacked website and the process that needs to be followed by an attacker.

II. Background

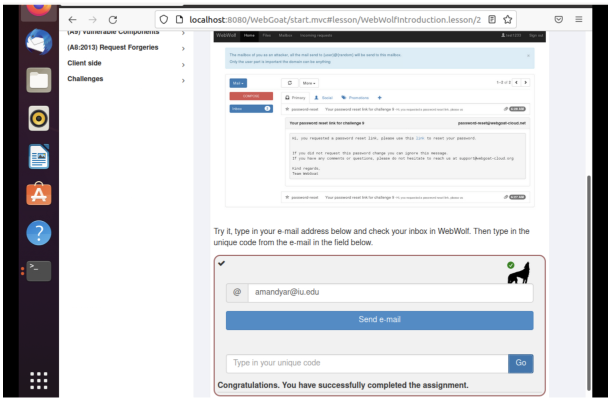
The Open Web Application Security Project (OWASP) Foundation strives to increase software security through community-led open source software projects, tens of thousands of members, hundreds of chapters worldwide, and local and international conferences. WebGoat and WebWolf are maintained by the Open Web Application Security Project (OWASP)

III. WebGoat

The purpose of OWASP WebGoat is to test Java-based applications for common web application vulnerabilities. It is a purposefully unsafe online application. This helps developers to be aware of the vulnerabilities so that they can design applications that are less prone to these vulnerabilities.The WebGoat can be installed in two ways through Docker and the other way via standalone. A typical server-side application issue is illustrated by WebGoat. The activities are meant to be used as a learning tool for penetration testing and application security.

IV. WebWolf

A different web program called WebWolf imitates an attacker's computer. It allows us to distinguish clearly between what occurs on the website that is being attacked and the steps you must do in your capacity as a attacker. WebWolf is has various services that it can provide such as hosting a file, receiving emails and landing page for incoming requests. The WebWolf provides the information of the request by controlling the incoming requests so that it can act as the landing page. This way we can retrieve information of users by allowing them to send requests, for example by sending them a password reset link through which we can intercept their request and collect their information such as the password Lab-Tasks: receiving email (fig-1), tricking user with reset password (fig-2)



localhost:8080/WebGoat/start.mvc#lesson/WebWolfIntroduction.lesson/2

The mailbox of you as an attacker, all the mail send to {user}@{random} will be send to this mailbox.
Only the user part is important the domain can be anything

password-reset Your password reset link for challenge 9 -Hi, you requested a password reset link, please us 6:28 AM

Your password reset link for challenge 9 password-reset@webgoat-cloud.net

```
Hi, you requested a password reset link, please use this link to reset your password.

If you did not request this password change you can ignore this message.
If you have any comments or questions, please do not hesitate to reach us at support@webgoat-cloud.org

Kind regards,
Team WebGoat
```

password-reset Your password reset link for challenge 9 -Hi, you requested a password reset link, please us 6:27 AM

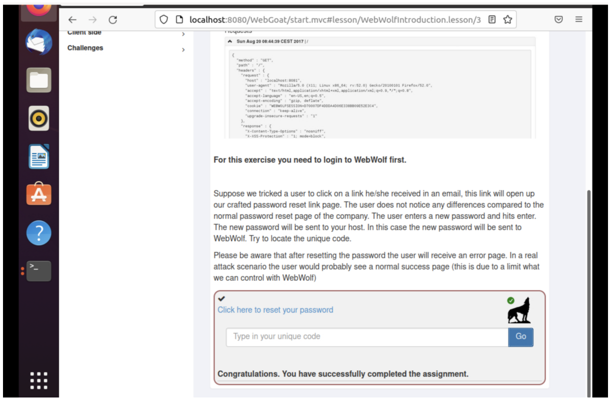
Try it, type in your e-mail address below and check your inbox in WebWolf. Then type in the unique code from the e-mail in the field below.

@ amandyar@iu.edu

Type in your unique code

Congratulations. You have successfully completed the assignment.

Fig. 1. receiving an email and entering the Unicode from the email



localhost:8080/WebGoat/start.mvc#lesson/WebWolfIntroduction.lesson/3

Sun Aug 20 08:44:39 CEST 2017 | /

```
{
  "method" : "GET",
  "path" : "/",
  "headers" : {
    "request" : {
      "host" : "localhost:8081",
      "user-agent" : "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0",
      "accept" : "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8",
      "accept-language" : "en-US,en;q=0.5",
      "accept-encoding" : "gzip, deflate",
      "cookie" : "WEBWOLFSESSION=D70007DF4DDDA4D06E3388B09E52E3C4",
      "connection" : "keep-alive",
      "upgrade-insecure-requests" : "1"
    },
    "response" : {
      "X-Content-Type-Options" : "nosniff",
      "X-XSS-Protection" : "1; mode=block",
```

For this exercise you need to login to WebWolf first.

Suppose we tricked a user to click on a link he/she received in an email, this link will open up our crafted password reset link page. The user does not notice any differences compared to the normal password reset page of the company. The user enters a new password and hits enter. The new password will be sent to your host. In this case the new password will be sent to WebWolf. Try to locate the unique code.

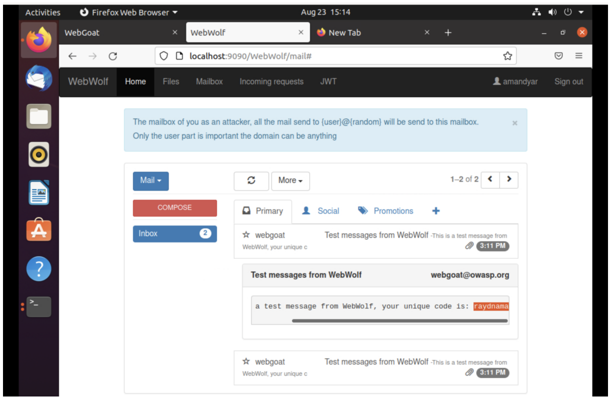
Please be aware that after resetting the password the user will receive an error page. In a real attack scenario the user would probably see a normal success page (this is due to a limit what we can control with WebWolf)

Click here to reset your password

Type in your unique code

Congratulations. You have successfully completed the assignment.

Fig. 2. sending an user the reset password link and retrieving their password



localhost:9090/WebWolf/mail#

The mailbox of you as an attacker, all the mail send to {user}@{random} will be send to this mailbox.
Only the user part is important the domain can be anything

webgoat Test messages from WebWolf -This is a test message from WebWolf, your unique c 3:11 PM

Test messages from WebWolf webgoat@owasp.org

```
a test message from WebWolf, your unique code is: raydnama
```

webgoat Test messages from WebWolf -This is a test message from WebWolf, your unique c 3:11 PM

Fig. 3. receiving the Unicode

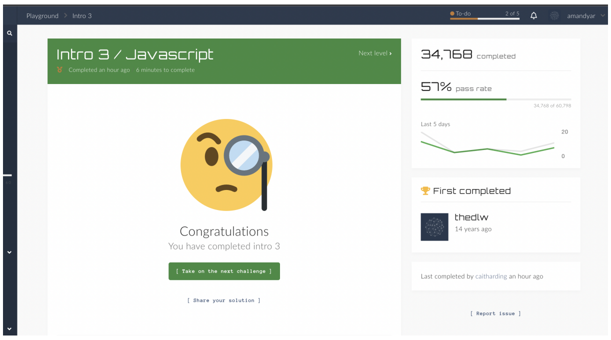
Advisor: Luyi Xing, Jiale Guan .

V. Environment Set-Up

Started of by creating a virtual environment using the virtual machine, which can be used to house the insecure application. 4096 Mb RAM, 2 CPU and 50 GB disk resources were dedicated for it to perform well. The operating system being used in the virtual machine is Ubuntu 20.04.4 (Desktop version).

VI. Bonus Task: Intro-3

The Task required me to find the password and it said JavaScript. Started by viewing the page source. Looked for passwords, I found a function that was comparing if the password is correct or incorrect. In the comparison statement there was a variable correct that was being used to compare. I searched for the variable correct and where it was declared. I found the variable correct along with its value and used the value to complete the challenge.



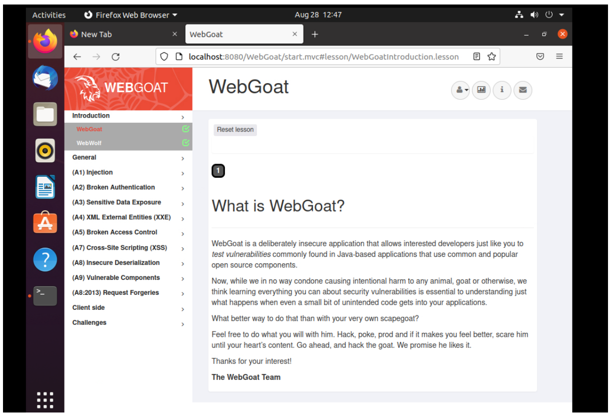
Congratulations
You have completed intro 3

Last completed by caitharding an hour ago

Fig. 4. Bonus Task completion screenshot Intro:3

VII. Conclusion

There is a huge learning curve and scope related to knowledge related to security. The WebGoat and WebWolf serves its purpose by helping understand the attacks and vulnerabilities at the most basic level. The WebWolf also gives a clear picture about the attackers environment that is being used, it also incorporates the variegated steps the attacker might take to accomplish the designated attacks.


Activities
Firefox Web Browser
Aug 28 12:47
New Tab
WebGoat
localhost:8080/WebGoat/start.mvc#lesson/WebGoatIntroduction.lesson
WEBGOAT
WebGoat
Introduction
WebGoat
WebWolf
General
(A1) Injection
(A2) Broken Authentication
(A3) Sensitive Data Exposure
(A4) XML External Entities (XXE)
(A5) Broken Access Control
(A7) Cross-Site Scripting (XSS)
(A8) Insecure Deserialization
(A9) Vulnerable Components
(A8:2013) Request Forgeries
Client side
Challenges
Reset lesson
1

What is WebGoat?

WebGoat is a deliberately insecure application that allows interested developers just like you to *test vulnerabilities* commonly found in Java-based applications that use common and popular open source components.

Now, while we in no way condone causing intentional harm to any animal, goat or otherwise, we think learning everything you can about security vulnerabilities is essential to understanding just what happens when even a small bit of unintended code gets into your applications.

What better way to do that than with your very own scapegoat?

Feel free to do what you will with him. Hack, poke, prod and if it makes you feel better, scare him until your heart's content. Go ahead, and hack the goat. We promise he likes it.

Thanks for your interest!

The WebGoat Team

Fig. 5. All Tasks Completed screenshot(Both WebGoat and WebWolf)

References

[1] https://github.com/WebGoat/WebGoat
[2] https://owasp.org/