Offensive Security using Burp suite

Author: Jose Torres
Advisor: Dr. Jeffrey Duffany
Department of Electrical, Computer Engineering and Computer Science

Abstract

Burpsuite is a tool used most professional web page pen tester. It had many features to help the pen tester do his job. The tool help student learn about different type of vulnerabilities like web cache poisoning, SQL injection, cross-site scripting (xss), and clickjacking attacks. Cross-site scripting (XSS) is a type of security vulnerability typically found in web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. Clickjacking (classified as a User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a user into clicking on something different from what the user perceives, thus potentially revealing confidential information or allowing others to take control of their computer while clicking on seemingly innocuous objects, including web pages. SQL injection is a code injection technique, in which malicious SQL statements are inserted into an entry field for execution.

Introduction

Burpuite is a collection of tightly integrated tools that allow effective security testing of modern-day web applications, the tool is written in java language basically the tool is cross-platform, Kali Linux already have Burp Suite Installed on their OS image. All other tool like intercepting traffic, brute forcing, etc is available on the free version but you cannot save your work, but the community version is great to start learning.

Background

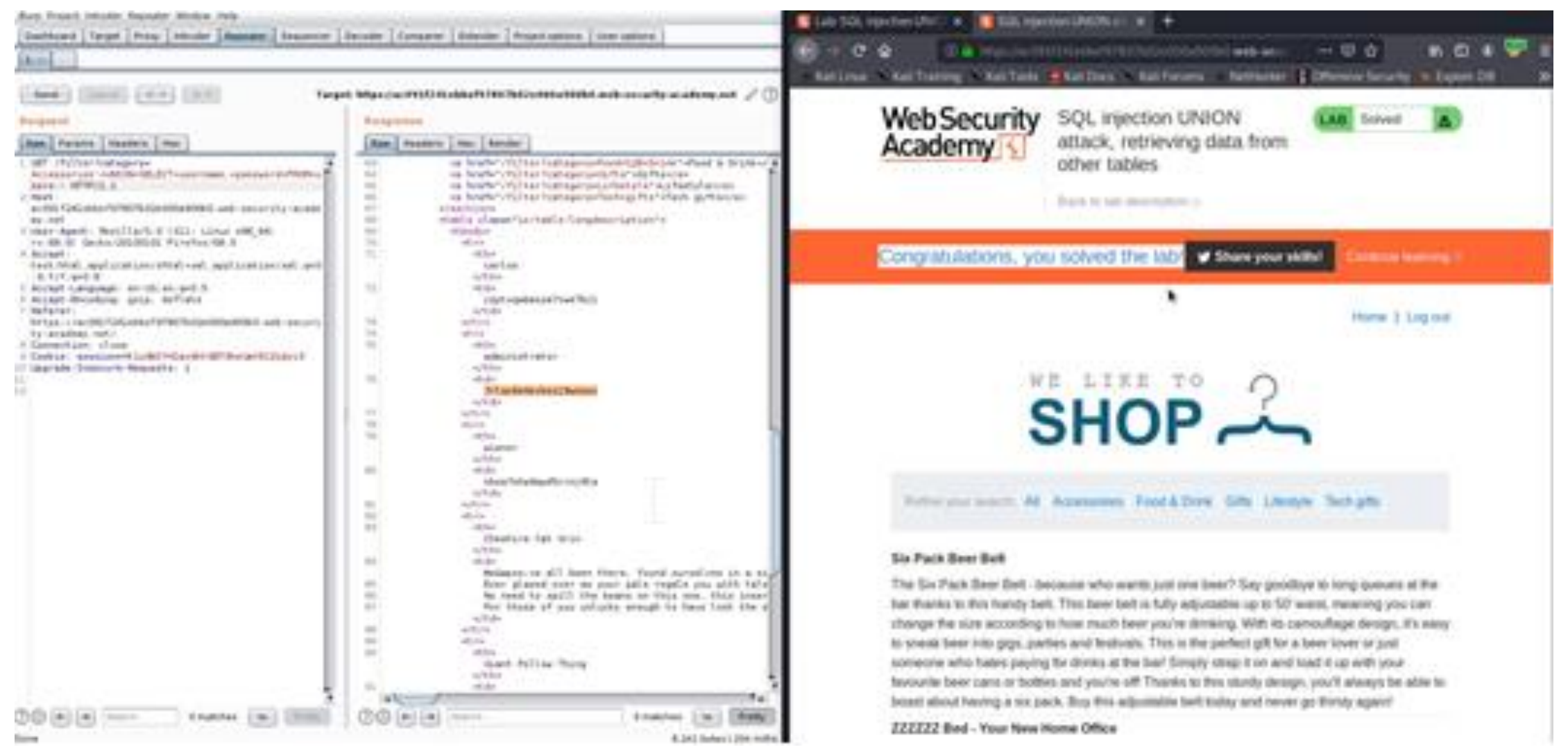
It requires some small knowledge of CSS, sql and network. Also some knowledge about computer security, network security and Linux (you can use windows to, but Linux is recommended for lab use). Network security consists of the policies and practices adopted to prevent and monitor unauthorize access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Computer security, the protection of computer systems and information from harm, theft, and unauthorized use. Computer hardware is typically protected by the same means used to protect other valuable or sensitive equipment, namely, serial numbers, doors and locks, and alarms. The protection of information and system access, on the other hand, is achieved through other tactics, some of them quite complex.

Problem

Cyber criminals are increasing but there less cyber security professional on the defensive and offensive side. This project shows how to start on offensive security using a tool called Burpsuite.

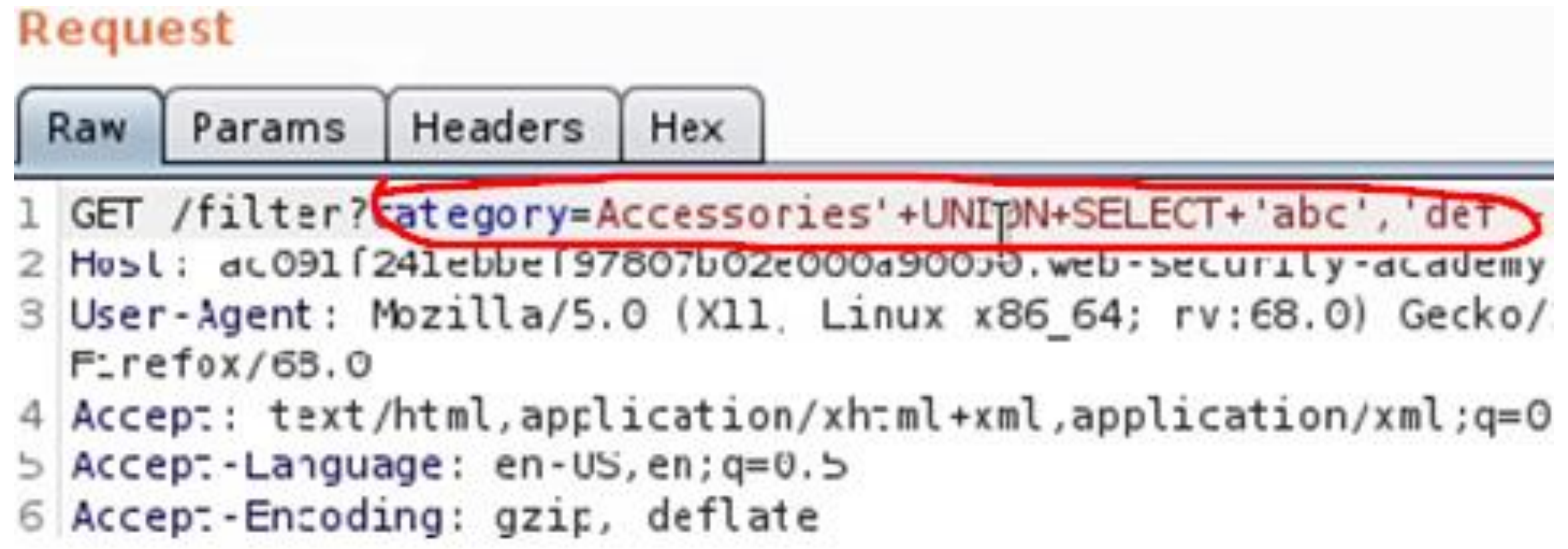
Methodology

We present the most common vulnerability and use https://portswigger.net/web-security academy to test these vulnerabilities legally like Web Cache Poisoning, SQL Injection, Cross-site scripting (XSS), Clickjacking and Access control vulnerabilities and privilege escalation. Each lab is done using Burpsuite Comunnity version on Kali Linux. The Portswigger academy have all the labs to practice legally and to evaluate burpsuite functionalities. Also each labs show what type a vulnerabilities have that website (lab) then you start experimenting on the websites until you find the solution using burpsuite, at the end of each labs it shows a confirmation screen.


Web Security Academy
SQL injection UNION attack, retrieving data from other tables
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Home | Log out
WE LIKE TO SHOP
Six Pack Beer Belt
ZZZZZZ Bed - Your New Home Office

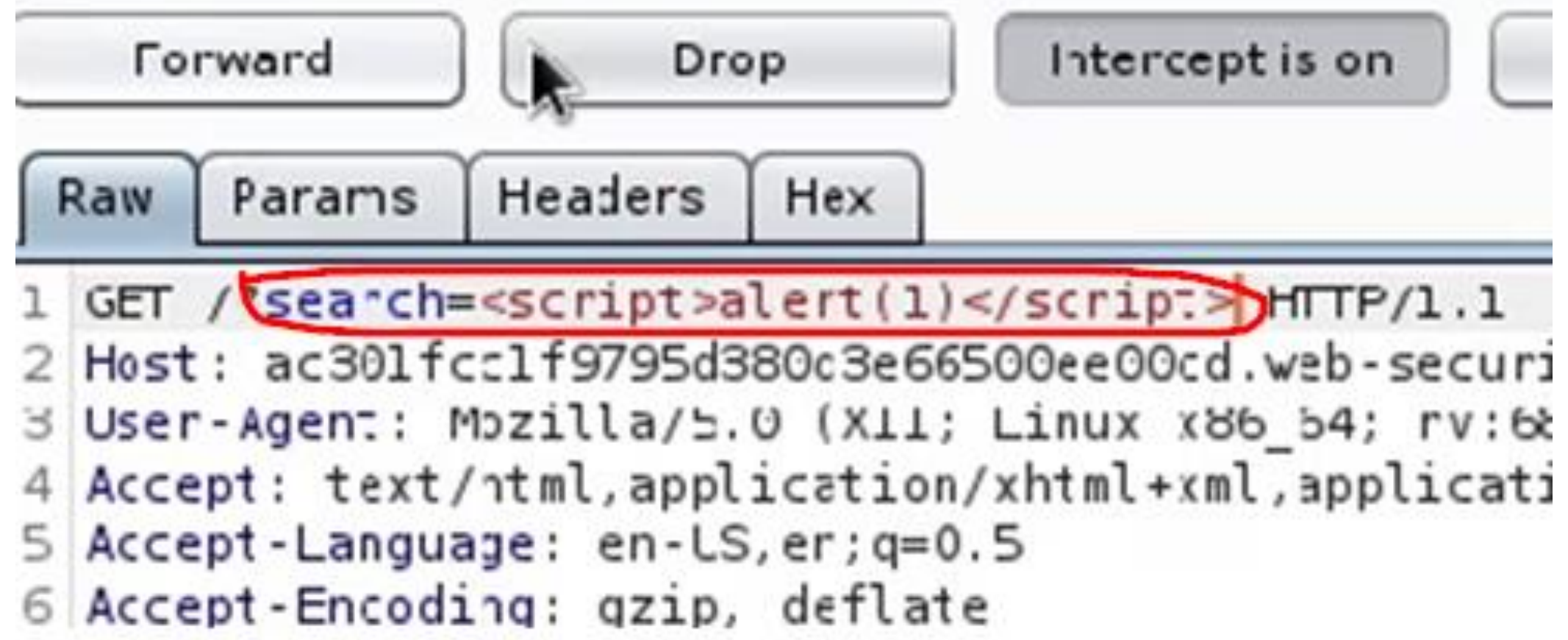
Example side by side burpsuite with firefox browser

Results and Discussion



```
GET /filter?category=Accessories'+UNION+SELECT+'abc','def
Host: ac091f241ebbef97807b02e000a90050.web-security-academy
User-Agent: Mozilla/5.0 (X11, Linux x86_64; rv:68.0) Gecko/
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

This image is an example of a SQL injection, in the marked area you can see a sql command using UNION SELECT, that line of sql is printed out all the websites user account with their password.

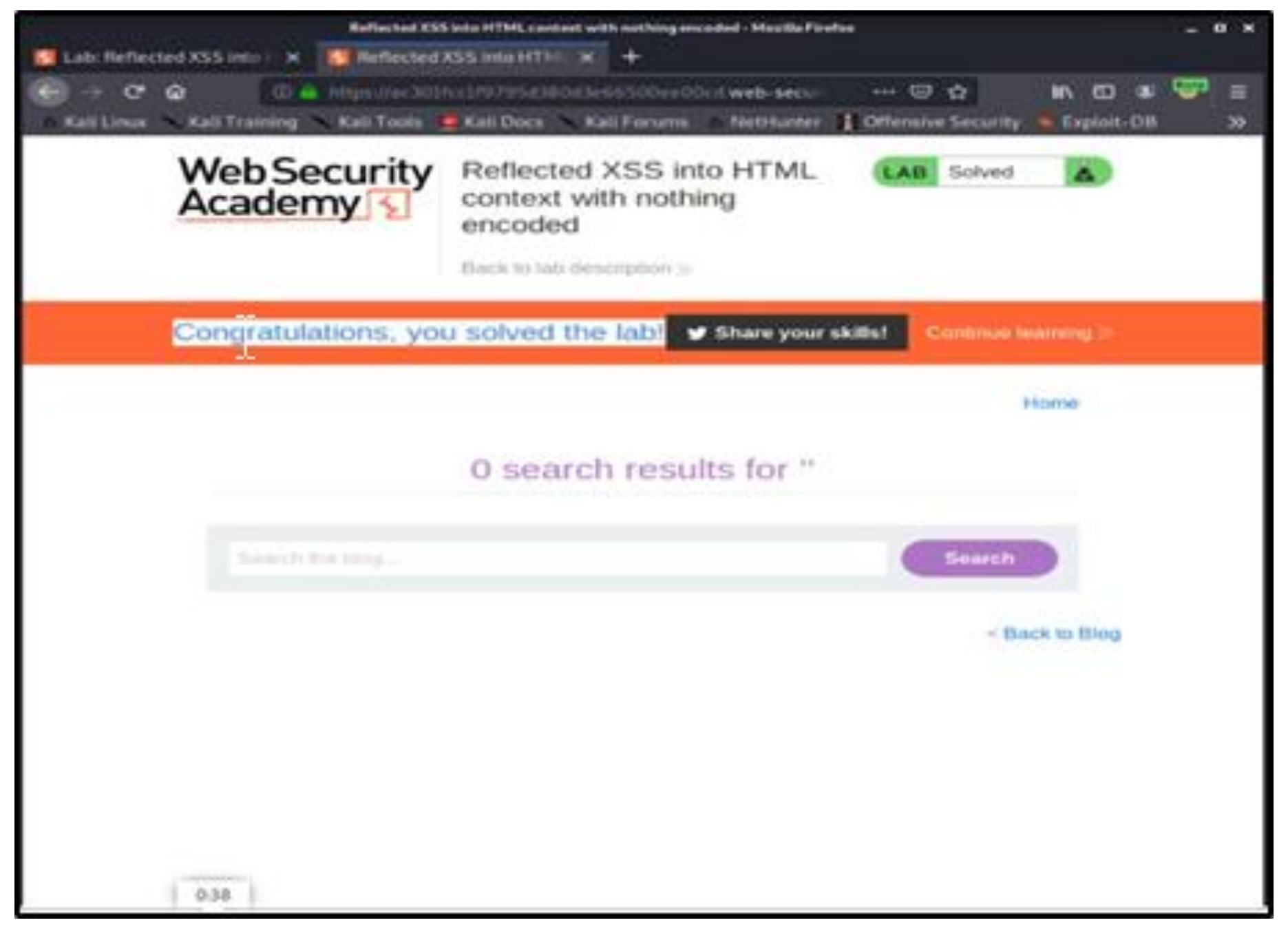


```
GET /?search=<script>alert(1)</script> HTTP/1.1
Host: ac301fcc1f9795d380c3e66500ee00cd.web-securi
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68
Accept: text/html,application/xhtml+xml,applicati
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

This image shows an example of a cross-site scripting (XSS), the marked area shows a JavaScript code that open an alert box on the victim's browser.

Results and Discussion

Each labs was done completed according to each lab specification. Burpsuite help a lot with web site pen testing and to start on this field. Although it had some trouble because burpsuite is a proxy server so the web browser must be configured to allow burpsuite intercept the websites. The community version of burpsuite is good to start but the pro version is recommended because it provide faster web intercepting and a vulnerability scan (the free doesn't have a vulnerability scan). But for this project the community version worked just fine.



Congratulations, you solved the lab!

0 search results for ''

Confirmation screen of a lab

Web cache poisoning is an advanced technique whereby an attacker exploits the behavior of a web server and cache so that a harmful HTTP response is served to other users. This technique involves two phases, the attacker must work out how to elicit a response from the back-end server that inadvertently contains dangerous payload. SQL Injection it is a vulnerability that allow the hacker to use queries of the application that makes to its database. Is mostly known as an attack vector for websites but can be used to attack any type of SQL database. SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server. The attacker can get the data that is not normally retrieve like data obliging to other users or access credential for the application. Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. It allows an attacker to circumvent the same origin policy, which is designed to segregate different websites from each other. Cross-site scripting carried out on websites accounted for roughly 84% of all security vulnerabilities documented by Symantec up until 2007. XSS effects vary in range from petty nuisance to significant security risk, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner network. Clickjacking is an interface-based attack in which a user is tricked into clicking on actionable content on a hidden website by clicking on some other content in a decoy website. Is an instance of the confused deputy problem, wherein a computer is innocently fooled into misusing its authority.

Conclusions

Burpsuite, a collection of integrated tools used most of web pen tester is a great tool to start pen testing, their website portswigger is great place to start learning and practicing legally like web cache poisoning, sql injection, cross-site scripting (XSS), clickjacking, and access control vulnerabilities and privilege escalation attacks. As you can see on this articles burpsuite mainly is use for intercepting website in order to analyze the traffic of the website, but it can be used to scan websites (pro version only), used payloads like brute forcing (community version works but the pro version is a lot faster), etc. We did not cover a lot of the labs because there are a lot of labs, but we cover the most important and common vulnerabilities using burpsuite and it has the necessary information to start on burpsuite and ethical hacking.

Future Work

Start making custom software (cyber security related) using python or other programming languages to keep growing as a computer scientist and cyber security professional.

Acknowledgements

I like to thanks my advisor Dr. Duffany for approving my project and editor Prof. Digna Delgado for checking my report.

References

[1] Akash Mahajan, “Burp Suite Essentials,” in Packt Publishing, Birmingham, United Kingdom, 2014, chap. 1

[2] Port Swigger Academy Web Cache Poisoning , Available: https://portswigger.net/web-security/web-cache poisoning/

[3] Port Swigger Academy SQL Injection learning material, https://portswigger.net/web-security/sql-injection

[4] Port Swigger Academy cross-site scripting learning material, https://portswigger.net/web-security/cross-site-scripting

[5] Port Swigger Academy clickjacking learning material, https://portswigger.net/web-security/clickjacking

[6] Port Swigger Academy Access control vulnerabilities and privilege escalation learning material, https://portswigger.net/web-security/access-control

[7] XSS https://en.wikipedia.org/wiki/Cross-site_scripting

[8] Clickjacking https://en.wikipedia.org/wiki/Clickjacking

[9] SQL Injection https://en.wikipedia.org/wiki/SQL_injection