Network Security Theory and Practice

Lab 02

Due April 13, 2021

POLICIES:

1. Coverage

File upload vulnerability, file inclusion vulnerability, SQL injection attack

2. Grade

All lab assignments account for 10% of the final grade

3. Individual or Group

Individual based, but group discussion is allowed and encouraged

4. Academic Honesty

Violation of academic honesty may result in a penalty more severe than zero credit for an assignment, a test, and/or an exam.

5. Submission

Soft copy of report.pdf on course.zju.edu.cn

6. Late Submission

20% deduction for late submission till April 17, 2021;
Deduction ceases upon zero;
Late submissions after April 17 23:59 will NOT be graded.

PREPARATION:

1. Lab Goal

Lab 02 aims to practice techniques that exploit file upload vulnerability, file inclusion vulnerability, and SQL injection.

Unrestricted file upload is a serious vulnerability that can have a detrimental effect on web application because we know that the file uploading feature allows us to upload documents according to the server, but if the file uploading facility is vulnerable then attacker can upload any malicious file on the web application, deface the website or gain access of the file system through a web shell.

File inclusions are part of every advanced server side scripting language on the web. They are needed to keep web applications' code tidy and maintainable. They also allow web applications to read files from the file system, provide download functionality, parse configuration files and do other similar tasks. Though if not implemented properly, attackers can exploit them and craft a LFI attack which may lead to information disclosure, cross-site-Scripting (XSS) and remote code execution (RFI) vulnerabilities.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).[1] SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection 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.

2. Recommended Tools

Burp Suite

Burp Suite supports reviewing/editing the data sent and received among other things. It functions as a proxy, typically configured to listen on 127.0.01 loopback address. An application such as a web browser or sqlmap is configured to use Burp Suite as a Proxy. This enables the review/editing of what is transmitted and received. Here is a link to a tutorial.

sqlmap

The tool of sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

LAB REQUIREMENTS:

Please carefully read the references before solving the following challenges. Hints are omitted if they can be found therein, thanks.

1. **https://2019.actf.lol/challenges#file%20inclusion1**
   hints:
   modify link to trigger an error message
   pay attention to the error message
2. **https://2019.actf.lol/challenges#file%20inclusion2**
   hints:
   in reference
3. **https://2019.actf.lol/challenges#Upload1**
   hints:
   craft command into a php file
   change the extension to impersonate an image file
   modify the extension back to php while transmission with Burp
4. **https://2019.actf.lol/challenges#Upload2**
   hints:

as hints for requirement 3
in reference

5. **https://2019.actf.lol/challenges#Upload3**
   hints:
   craft php file with image header format
6. **https://zjusec.com/play?q=16**
   hints:
   in reference

REPORT REQUIREMENTS:

1. **Report Template**
   NetSec-Lab-Report-Template.doc
2. **Language**
   English
3. **Content Highlights**
   For each of lab requirements 1~5, please use screenshots to showcase the correct processes for solving each challenge.
   For certain steps, necessary discussions may be provided to demonstrate your understanding.
4. **Page Limit**
   Please keep the report as concise as possible.
5. **References**
   File inclusion vulnerability:
   https://blog.csdn.net/Vansnc/article/details/82528395
   File upload vulnerability:
   https://blog.csdn.net/wy_97/article/details/76549761
   https://blog.51cto.com/dearch/1828635
   SQL injection:
   https://www.cnblogs.com/Vinson404/p/7253255.html