Analyzing Vulnerabilities - Workshop

SoftUni Team

Technical Trainers

Software University

SoftUni

Software University

https://softuni.bg

Have a Questions?

Software University

sli.do

#Cyber_Security

Table of Contents

Understanding Vulnerabilities

Understanding Vulnerabilities

Software University

- **Vulnerabilities** on their core, are poorly written code
- The better you are with coding, the more you can understand everything
- They are core concept in cyber security
- On one hand side they must be **mitigated** / **patched**, on other they must be exploited
- Vulnerabilities can arise from literally everywhere! Never think like "**there is no way that is going to work**", guess what, it is a way! Try it out!

Do not Overcomplicate Things!

Software University

- Yes, indeed there are twisted vulnerabilities, but as beginners, start understanding the basic ones
- In this workshop we will examine the following **vulnerabilities**:
  - SQL Injection
  - Cross Site Scripting (**XSS**)
  - OS Command Injection
  - Directory Traversal
  - Access Control
  - File Upload

Understanding SQL Injection

- SQL injection is vulnerability, allowing user to interfere with the database engine, corrupting and modifying queries
- There are many types of **SQL injections**, but for simplicity we will focus on the very basic ones
- Lab Link:
  - *https://portswigger.net/web-security/sql-injection/lab-retrieve-hidden-data*

Understanding XSS

- XSS is vulnerability, allowing user to inject and execute custom javascript
- This attack can be weaponized as client-side attacks
- There are three types of **XSS**, reflected, stored and **DOM** based
- Lab Link:
  - *https://portswigger.net/web-security/cross-site-scripting/reflected/lab-html-context-nothing-encoded*

Understanding OS Command Injection

Software University

- OS Command Injection is vulnerability, allowing user to inject custom OS commands
- This attack can be weaponized mainly for C2
- Lab Link:
  - *https://portswigger.net/web-security/os-command-injection/lab-simple*

Understanding Directory Traversal

Software University

- Directory Traversal is vulnerability, allowing user to read local files stored on the operational system (OS)
- Even though this looks similar to LFI (Local File Inclusion), the difference is that LFI can execute files, while DT can only read
- Lab Link:
  - *https://portswigger.net/web-security/file-path-traversal/lab-simple*

Understanding Access Control Vulnerabilities

Software University

- Access Control vulnerabilities, are type of vulnerabilities that allows an attacker to view and interact with resources, that initially he was missing permissions for
- In other words, access and work with resources, by bypassing access control restrictions
- Lab Link:
  - *https://portswigger.net/web-security/access-control/lab-unprotected-admin-functionality*

Understanding File Upload Vulnerabilities

Software University

- File Upload vulnerabilities, allows an attacker to upload (and execute in best case for the pentester) malicious files, most oftenly for obtaining C2
- The problem here is that there is no system for validating the uploaded files
- Lab Link:
  - *https://portswigger.net/web-security/file-upload/lab-file-upload-remote-code-execution-via-web-shell-upload*

Code Reviewing Exploits

Pluck CMS 4.7.13 – File Upload RCE (Remote Code Execution) (Authenticated)

Software University

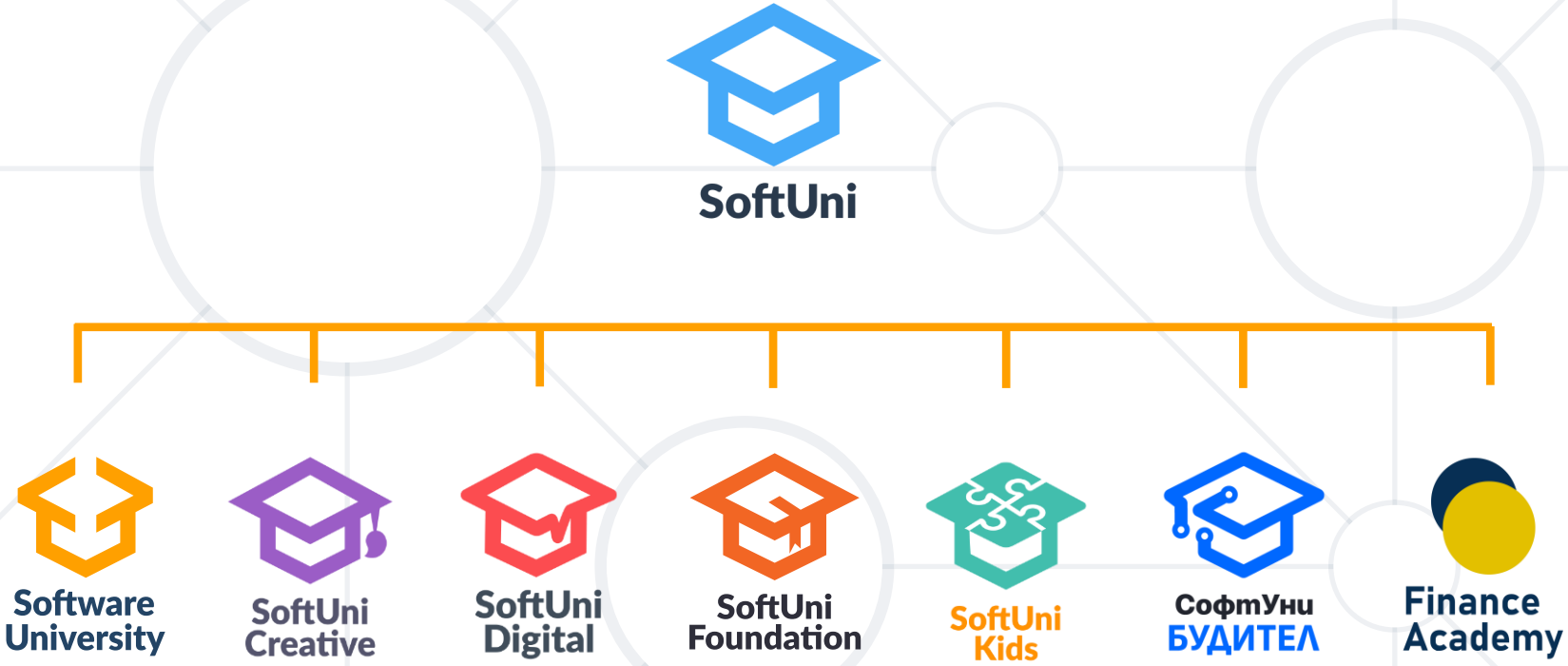
- This exploit (*https://www.exploit-db.com/exploits/49909*) is performing the following actions:
  - Authenticating
  - Uploading File
  - Executing the File
- Let's examine it

Summary

Software University

- Understanding Vulnerabilities
  - Understanding SQL Injection
  - Understanding XSS
  - Understanding OS Command Injection
  - Understanding Directory Traversal
  - Understanding Access Control Vulnerabilities
  - Understanding File Upload Vulnerabilities
- Code Reviewing Exploits

Questions?



SoftUni Diamond Partners

Software University

SmartIT

Coca-Cola HBC Bulgaria

SUPER HOSTING .BG

createX

Postbank

Решения за твоето утре

DRAFT KINGS

THE CROWN IS YOURS

VIVACOM

AMBITIONED

INDEAVR

Serving the high achievers

PHAR VISION

Trainings @ Software University (SoftUni)

- Software University – High-Quality Education, Profession and Job for Software Developers
  - softuni.bg, about.softuni.bg
- Software University Foundation
  - softuni.foundation
- Software University @ Facebook
  - facebook.com/SoftwareUniversity

License

- This course (slides, examples, demos, exercises, homework, documents, videos and other assets) is **copyrighted content**
- Unauthorized copy, reproduction or use is illegal
- © SoftUni – https://about.softuni.bg/
- © Software University – https://softuni.bg