Name: ..
Date: ..
Org: ..

Pentest Report

Vulnerabilityanalys of XXXXXX

Summary

A penetrationtest was conducted and the following vulnerabilities were discovered...xss,lfi,rfi, continue the summary...

xss

The XSS vulnerability is due to the fact that the user-agent string is not sanitized before being passed to the vulnerable script. This is a common issue in XSS attacks.

The following is an example of the vulnerability:

<script>alert(document.cookie)</script>

This is a simple XSS attack, but it can be used to read cookies, session cookies, and other sensitive data from the browser.

The vulnerable script is located in the /plugins/jquery/jquery-1.7.2.min.js file. The vulnerable code is as follows:

var cookie_name = 'jquery-cookie-test'; var cookie_value = '<script>alert(document.cookie)</script>';

If the user-agent string contains the characters '<', '>', ',', '&', '"', ';', '"' and '/', then the vulnerable script is executed.

lfi

The LFI vulnerability is due to the fact that the user-agent string is not sanitized before being passed to the vulnerable script. This is a common issue in LFI attacks.

The following is an example of the vulnerability:

<script>alert(document.cookie)</script>

This is a simple LFI attack, but it can be used to read cookies, session cookies, and other sensitive data from

Methodology

The Penetration Testing Execution Standard (PTES) is a detailed guide for conducting penetration tests, created by security experts. It standardizes testing methods, helping security professionals and businesses. It covers testing from planning to reporting, and emphasizes a tailored approach for each organization's needs. The PTES improves penetration testing effectiveness.

Pre-engagement Interactions

This is the preparation phase for the pen test. It is all about document approvals and tools needed for the test.

Intellegence Gathering

In this phase information about the target system are gathered from external sources like social media websites, official records etc. This phase comes under OSINT (Open-Source Intelligence).

Threat Modelling

It is a procedure for optimizing network security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system. It is skipped in typical pan tests.

Vulnerability Analysis

This phase discovers and validates vulnerabilities.That is risk that an attacker could exploit and gain authorized access to the system or application.

Exploitation

In this phase, the tester try to reach the security of the target system using the vulnerabilities previously identified and validated.

Post Exploitation

This phase maintains the control over target system and collects data.

Reporting

Documents entire process in a form understandable to the client.

Results

Result presents all the findings, how, and why the finding was discovered. Results also presents if the discovered vulnerability is a threat.

Recommendations

Recommendations presents all the recommendations for mitigating and avoiding these types of vulnerabilities.

XSS (Cross-Site Scripting)

How to prevent XSS (Cross-Site Scripting) attacks?

I've been learning about XSS attacks and how they work since the beginning of the year. This is the first time I'm trying to write a blog post about it.

So, I will try to explain how XSS attacks work, and how to prevent them, in this post.

Let me start by defining what XSS is.

What is XSS?

In short, XSS is the process of injecting malicious script or HTML into a website.

The word "XSS" means "Cross-Site Scripting".

Let me explain with an example.

Let's say you visit a website and you see the following text:

<script>alert(document.cookie);</script>

It is a simple example. But the example is not very good.

If you want to get a better example, you can try:

<script>alert(document.cookie);</script>

You might have noticed that the above example is vulnerable to XSS attacks.

What are XSS attacks?

XSS attacks are similar to SQL injections and are not

LFI (Local File Inclusion)

How to prevent LFI (Local File Inclusion) attacks?

In this post, we will describe how to prevent LFI attacks. LFI attacks are security vulnerabilities in software that allow attackers to exploit code running on a targeted computer. For example, you

can exploit the vulnerability by running a malicious program on a computer you control.

What is LFI?

LFI attacks are similar to other security vulnerabilities. They are security vulnerabilities that can be exploited by malicious code. In other words, LFI attacks are similar to buffer overflows and heap overflows.

In the case of buffer overflows, an attacker can exploit the buffer overflow by sending a malicious program that contains a buffer overflow into a buffer. The buffer overflow will cause the program to crash. This is the most common kind of LFI attack.

In the case of heap overflows, the attacker can exploit the heap overflow by sending a malicious program that contains a heap overflow into a heap. The heap overflow will cause the program to crash. This is the most common kind of LFI attack.

The difference between the buffer overflow and heap overflow is that the buffer overflow can be exploited only by malicious code, while the heap overflow can be exploited by malicious code and also by benign code.

RFI (Remote File Inclusion)

How to prevent RFI (Remote File Inclusion) attacks?

The most common form of RFI (Remote File Inclusion) attack involves the use of a malicious web site that contains malicious code (also known as remote code execution). This is done to gain unauthorized access to a vulnerable program, or to install a malicious program on your computer.

The web site may also be used to create a back door (i.e., a way to gain access to your computer) by infecting your browser with malware.

The following article discusses how to protect against RFI attacks and also describes how to detect them.

How to detect RFI attacks?

The most common form of RFI attacks involves the use of a malicious web site that contains malicious code (also known as remote code execution). This is done to gain unauthorized access to a vulnerable program, or to install a malicious program on your computer.

The web site may also be used to create a back door (i.e., a way to gain access to your computer) by infecting your browser with malware.

The following article discusses how to protect against RFI attacks and also describes how to detect them.

How to prevent RFI attacks?

There are many steps you can