Attack Case Study

Adult Friend Finder (2016)

Affected Parties: Over 412 million user's information compromised.

Usernames, Email addresses and Passwords.

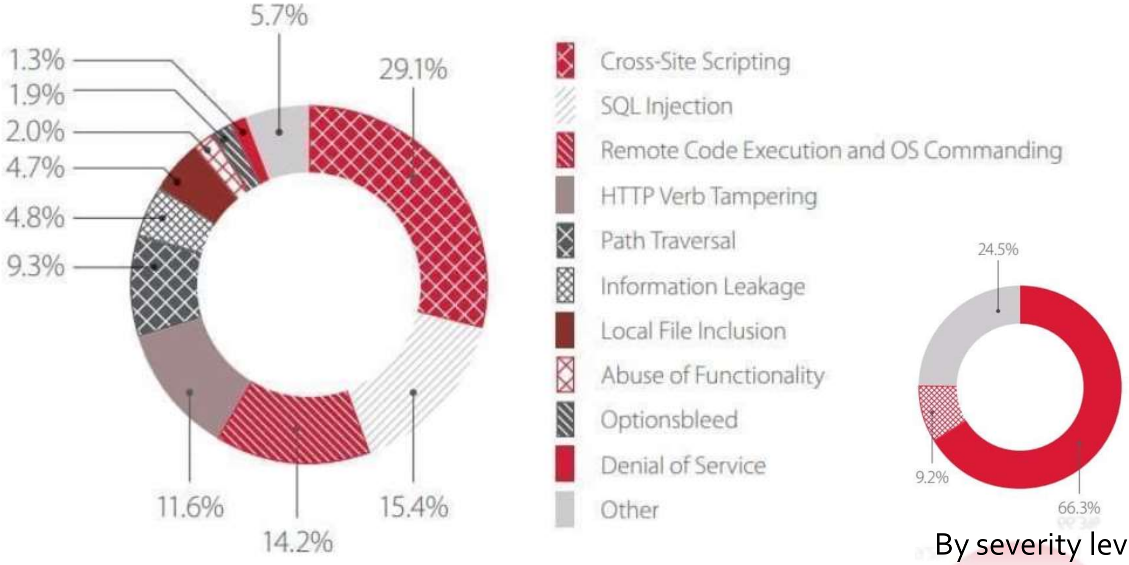
Attack Category

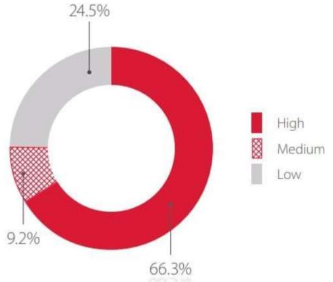
LFI - Local File Inclusion

An attacker can use Local File Inclusion (LFI) to trick the web application into exposing or running files on the web server. An LFI attack may lead to information disclosure, remote code execution, or even Cross-Site-Scripting (XSS). Typically, LFI occurs when an application uses the path to a file as input. If the application treats this input as trusted, a local file may be used in the include statement.

Local File Inclusion is very similar to Remote File Inclusion (RFI) however, an attacker using LFI may only include local files (not remote files like in the case of RFI).

2016 Top Network Attacks





By severity level

FriendFinder.com is a group of adult websites which includes Penthouse.com, Cams.com, iCams.com and Stripshow.com and is largely focused on casual sexual encounters and pornography.

During October of 2016, the FriendFinder.com network was breached, with over 412 million user’s information being compromised.

The information included in the breach was contained within six databases published online and included usernames, email addresses and passwords.

Some of these passwords were stored within the database using plaintext, with the remainder stored using the SHA-1 hash function.

A majority of the accounts that were compromised used Hotmail, Gmail, and Yahoo! email addresses however, over 5,000 accounts were registered to accounts with .gov addresses and over 78,000 accounts were registered to accounts with .mil addresses.

One of the more shocking revelations of the breach was that it included over 15 million accounts that users had “deleted” from the website, showing that the organization was not purging data per customers wishes.

Timeline

Adult Friend Finder
LFI Attack 2016

1 The Friend Finder Network was breached sometime in mid-October 2016

2 Over 412 million user's information being compromised due to a LFI attack

3 Hackers collected 20 years of data on six databases. The three largest site's SQL databases included usernames, email addresses, and the date of the last visit, and passwords, which were either stored in plaintext or scrambled with the SHA-1 hash function.

4 The users from Adult Friend Finder declare to receive a lot of targeted spam emails ever since the leak

5 Many users declared the will to move forward to the court.

6 Friend Finders Network did disclose that they had been aware of vulnerabilities and had taken steps to correct them.

Vulnerabilities

Overall Summary

During October of 2016, the FriendFinder.com network was breached, with over 412 million user's information being compromised.

Vulnerability #1

Some of the passwords were stored within the database using plaintext.

Vulnerability #2

The databases were not well protected.

Vulnerability #3

Data in databases was over more than 20 years and security measures were not considered.

Vulnerability #4

Data that was encrypted was with outdated SHA-1 hash function.

Costs

- Lack of credibility
- Loss of users
- Multiple court processes
- Obsolete Cybersecurity procedures

Prevention

- Evaluation of the security and privacy policies.
- Early detection
- Maintain and update the databases.
- Critical patches
- Encryption
- Implement two-factor authentication