IHC 2018 .CAMP
ITALIAN HACKER CAMP

IMAGE-SHARING SITES AND STORED XSS

A serious problem

IHC 2018 .CAMP
ITALIAN HACKER CAMP

WHAT IS A CROSS-SITE SCRIPTING?

Cross-site scripting (XSS) is an attack that allows an attacker to inject malicious JavaScript code into a website (or web application) and run it on another user's browser.

XSS is often a vector: the attacker exploits a vulnerability in a website that the victim visits to execute a malicious JavaScript code in his browser.

IHC 2018 .CAMP
ITALIAN HACKER CAMP

TYPES OF XSS

- **Reflected**, the JavaScript code originates from the browser’s request
- **Persistent**, the Javascript code originates from the website's database

XSS ATTACK CONSEQUENCES

- **Cookie stealing**, an attacker can obtain the user's session cookies
- **Information gathering**, it is possible to know info about user's OS or browser and activate hardware components (like webcam or GPS)
- **Mining**, to use the victim's CPU to mine a cryptocurrency, by injecting a JavaScript code

IMAGE-SHARING SITES AS VECTORS

The idea is to use image-sharing sites as vectors: the images are a content that can become very viral (memes) on the Internet, and can be easily shared: forums, blogs, social networks, chats. So a stored XSS on an image-sharing site can reach a large number of people.

MOST COMMON WEAKNESSES

- **Input field**, for example album's title or image's caption
- **Filename**, it is possible to inject JavaScript code via image's filename
- **EXIF Data**, it is possible to inject code by editing these info of an image

INPUT FIELD

Input fields and forms are often vulnerable to XSS attacks, because there is no correct filter or escape. So it is possible to inject JavaScript code via album's title, image's title, image's caption, etc.

IHC 2018 .CAMP
ITALIAN HACKER CAMP

EXAMPLE OF BAD FILTER

INPUT <details open o***ontoggle="1"***ntoggle="confirm(1)">

OUTPUT <details open ontoggle="confirm(1)">

FILENAME

By using the image’s filename, an attacker can inject malicious code in a website if, while the file is being uploaded, its name doesn't get cleaned. On Windows file system (NTFS) it is **not** possible to use many special characters in the filename, but it is possible on macOS file system (NFS, NFS+) and Linux (ext[2-4]).

IHC 2018 .CAMP
ITALIAN HACKER CAMP

CHARACTERS ALLOWED

- On Windows (NTFS): any Unicode except NUL, \, /, :, *, ", <, >, |
- On macOS (HFS, HFS+): any Unicode except : or /
- On Linux (ext[2-4]): any byte except NUL or /

EXIF DATA

EXchangeable Image Format data in an image file (JPG) are descriptive meta-data about various information: date and time, geolocation, ISO, shutter, camera model, etc.

Some sites read and use EXIF data of the images, so, if there are no filters, it is possible to inject JavaScript code via EXIF data.

EXIFTOOL

An useful tool to edit EXIF data from command line is **ExifTool** by Phil Harvey.

EXAMPLE ./exiftool -Model='<xss_payload>' image.jpg

IHC 2018 .CAMP
ITALIAN HACKER CAMP

TIPS AND TRICKS #1

Always try the Android app! Sometimes it is possible to bypass the XSS protections by using the mobile app to inject Javascript code.

TIPS AND TRICKS #2

Always check a website on different devices! Often a website is different on different devices, and the difference is not just in design. So an injected JavaScript can run on mobile version of a website, but not on the Desktop version.

IHC 2018 .CAMP
ITALIAN HACKER CAMP

CONCLUSION

All examples are based on vulnerabilities found on some “big” image-sharing sites. These sites have over **5 million** likes on Facebook. The large number of people that these services can reach makes the security of these sites a serious issue.

IHC 2018 .CAMP
ITALIAN HACKER CAMP

BIBLIOGRAPHY