XSS (Cross-Site-Script) (Stored)

Cross-Site-Script is a potentially fatal attack in which a function not considered by the developer works by inserting script code such as JavaScript into a bulletin board or webmail. Thus, it is an attack targeting users.

When the XSS attack takes place

1. With frequent web requests, when data is entered into a web application through untrusted source code.
2. When you have dynamic content that transmits malicious content to web users whose data has not been verified

Stored XSS (AKA Persistent or Type 1)

Stored XSS generally occurs when user input is stored on the target server, such as in a database, in a message forum, visitor log, comment field, etc. And then a victim is able to retrieve the stored data from the web application without that data being made safe to render in the browser. With the advent of HTML5, and other browser technologies, we can envision the attack payload being permanently stored in the victim’s browser, such as HTML5 database, and never being sent to the server at all.

<Low>

스크린샷이(가) 표시된 사진

자동 생성된 설명

스크린샷이(가) 표시된 사진

자동 생성된 설명

스크린샷, 시계이(가) 표시된 사진

자동 생성된 설명 스크린샷이(가) 표시된 사진

자동 생성된 설명

Users can’t show the script contents on the board. Thus, if specific user confirms the board, the script code is automatically executed.

<Medium>

스크린샷이(가) 표시된 사진

자동 생성된 설명

medium.php

This code can’t use the script tag. Because there is a function where script tag is replaced with ‘’.

<High>

스크린샷이(가) 표시된 사진

자동 생성된 설명

This code can’t use the script tag. Because there is a function where script tag is replaced with ‘’.

스크린샷이(가) 표시된 사진

자동 생성된 설명

스크린샷이(가) 표시된 사진

자동 생성된 설명

As you see, you can attack through the img tag. If you use the various script code like this, the attacker can gain the cookie information of specific user.

\*Summary\*

After an attacker stores malicious code on the server using a board or pop-up window, it is to attack of data interception or malicious code installation without the user knowing by working whenever users open it.

<Security>

스크린샷이(가) 표시된 사진

자동 생성된 설명

If a programmer use the token, XSS Attack is impossible like this.