JS Deobfuscation

Super Quick Example

Quick Example

Go to competitivecyber.club/static/decode.html

Open Developer Console

Chrome/Firefox: Ctrl+Shift+J (or Cmd+Shift+J on a Mac

Chrome: F12

Internet Explorer: Drop out of Mason

Safari: Requires Setup (Prefences / Advanced / Show Develop menu in menu bar)

Look at the actual stuff

View source by right clicking on page and hitting view source

NOTICE THIS SHITSHOW

```
                // This problem can be solved in much simpler ways than
                // looking at the code below. Browser developer tools
                // are your friend.
                var d=
['\x74\x64\x3e','\x65\x20\x6e','\x67\x5f\x62','\x3c\x2f\x74','\x73\x20\x64','\x69\x6f\x76','\x63\x34\x34','\x61\x74\x69','\x36\x64\x65','\x65\x72\x79','\x61\x
72\x64','\x61\x72\x64','\x34\x63\x39','\x64\x3e\x3c','\x72\x6f\x62','\x63\x20\x61','\x6f\x6e\x20','\x39\x37\x64','\x35\x36\x33','\x73\x74\x61','\x6e\x74\x73',
'\x20\x44\x72','\x3e\x37\x2f','\x61\x31\x34','\x64\x69\x6f','\x72\x20\x63','\x6c\x6f\x70','\x20\x74\x68','\x63\x32\x62','\x33\x30\x34','\x33\x32\x63','\x66\x6
c\x61','\x69\x6e\x67','\x31\x30\x64','\x74\x64\x3e','\x75\x72\x67','\x6f\x74\x69','\x6e\x65\x72','\x33\x39\x38','\x34\x3c\x2f','\x75\x6c\x61','\x64\x3e','\x73
\x73\x69','\x65\x78\x74','\x2e\x20\x43','\x3c\x74\x64','\x6f\x66\x20','\x54\x6f\x77','\x3c\x2f\x74','\x3c\x2f\x74','\x74\x64\x3e','\x65\x76\x65','\x32\x31\x2f
','\x61\x6b\x65','\x64\x3e\x3c','\x20\x66\x6f','\x6c\x61\x75','\x61\x73\x63','\x20\x67\x65','\x32\x30\x31','\x33\x66\x61','\x72\x20\x73','\x3e\x44\x72','\x61\
x64\x30','\x3c\x74\x64'];var
m=d[64]+d[22]+d[52]+d[59]+d[39]+d[50]+d[45]+d[62]+d[44]+d[56]+d[24]+d[21]+d[53]+d[48]+d[13]+d[0]+d[47]+d[10]+d[4]+d[51]+d[26]+d[32]+d[27]+d[1]+d[43]+d[58]+d[3
7]+d[7]+d[16]+d[46]+d[14]+d[36]+d[15]+d[42]+d[19]+d[20]+d[55]+d[25]+d[11]+d[5]+d[57]+d[40]+d[61]+d[35]+d[9]+d[3]+d[54]+d[34]+d[31]+d[2]+d[17]+d[23]+d[12]+d[6]
+d[60]+d[38]+d[63]+d[18]+d[29]+d[8]+d[28]+d[30]+d[33]+d[49]+d[41];
                $('#contents').html(m);
                checker();
```

What's it doing?

Storing something in variable "m" (hence, "var m")
Storing something in variable "d" (hence, "var d")

What do we do about it?

In console, type "m", then enter, then "d" then enter to see what it is

Got the flag!

Cool, wanna see what it's actually doing?

http://jsbeautifier.org/ (feel free to use other deobfuscating/beautifying sites, or chain them)

Check whatever boxes apply (in this case "unescape printable….")

Other common deobf techniques

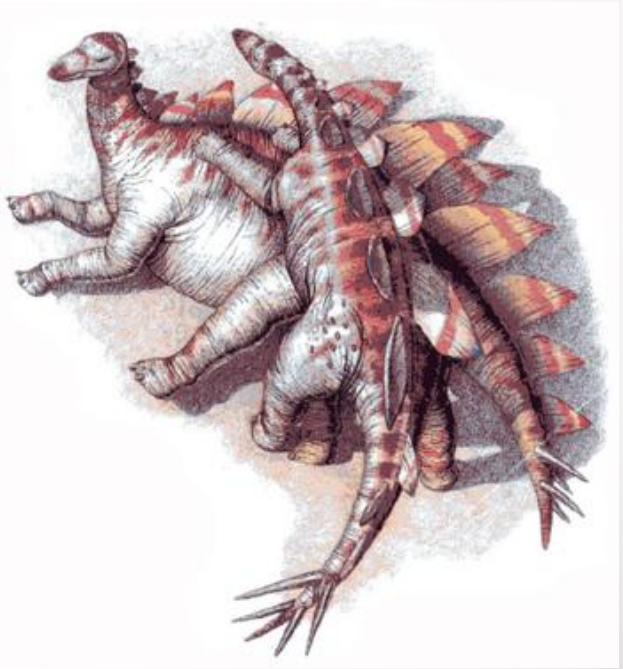
If it's doing something like "Decode this massive encoded blob, then execute it", change the function to "echo (display) it out" instead of execute and you have the decoded blob

Google for deobfuscators!

Steganography

What is Steganography?

- The practice of hiding messages in a way that nobody would even suspect there is a hidden message
- Different from cryptography
- In competition, usually means hiding a message in a JPG/GIF/PDF/MP3



JPG Analysis

- Hex Editor
  - Notepad++ extension on Windows
  - iHex on OSX (or hexdump command)
- FFD9 always at end of jpg
- Exif (Exchangeable image file format) data, which is basically metadata
  - Location Coordinates
  - Author
  - Camera model

GIF Analysis

- Look at it frame-by-frame
- OSX = use Preview
- May be combined with cryptography

PDF Analysis

- See if media (if PDF isn't "flat" is covering anything up
  - Redacted portions (blacked out areas)
- Look at it in hex editor or run strings

MP3 Analysis

- Listen to it
- Metadata
- Spectrum analysis

Compressed Data

- Sometimes a compressed archive will be renamed to something else, this can be identified with the **file** command
- This is generally done to defeat **strings.**
- Sometimes there will be compressed data embedded in another item. This is usually discoverable by **foremost.**
- Files include .tar,.tar.gz, .gz, .xz, .rar, .gzip, etc
- Magic bytes for a ZIP is PK = Phil Katz, inventor of the zip file format

Tools

- Hex Editors
  - Bless, iHex, extension for Notepad++
- Foremost
  - Automatically parses files for other files (available for Linux and OSX)
- Scalpel
  - More pointed version of Foremost
- Online tools for spectrum analysis or general steg tools (QuickSTego, Xiang)

Steps

- If don't know what a file is, look at it in a hex editor or run the file command
- Try unzipping it
- Look at exif data
- See if you can convert file to more useful format
- Open file in choice editor of that type
- Look to see if anything is unusual about the file

Remember

- Steganography challenges generally aren't the complicated ones in CTFs
- The hard part is knowing when it's steg and when it's something else

Challenge

- https://ctf.competitivecyber.club

- Don’t use any of your actual passwords for this
- You will be on a scoreboard