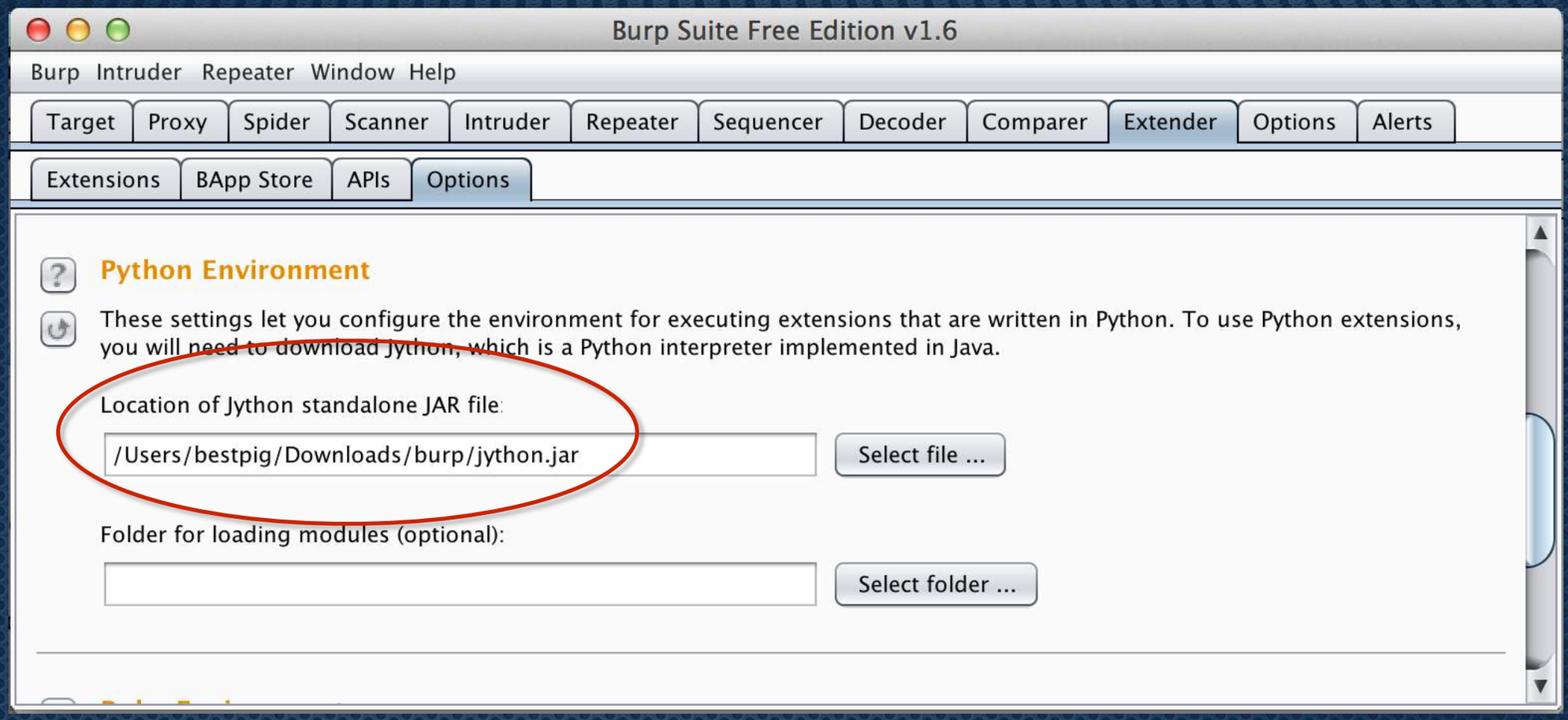
Burp Suite Plugin Practical

BestPig

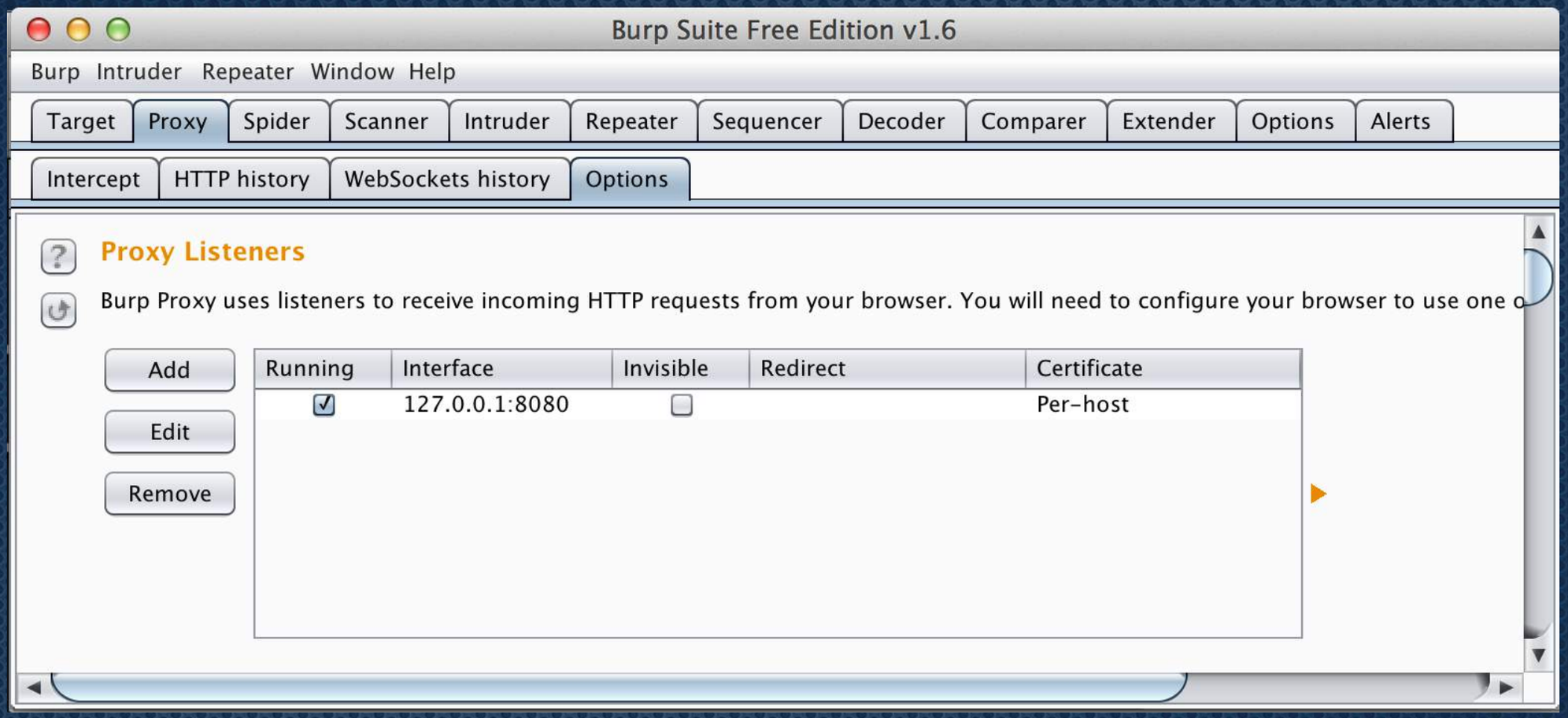
Download burp

- Get BURP 1.6:
  http://www.portswigger.net/burp/download.html
- Launch
  java -XX:MaxPermSize=1G -jar burpsuite_free_v1.6.jar

Configuring Jython



Setup the proxy



Skeleton

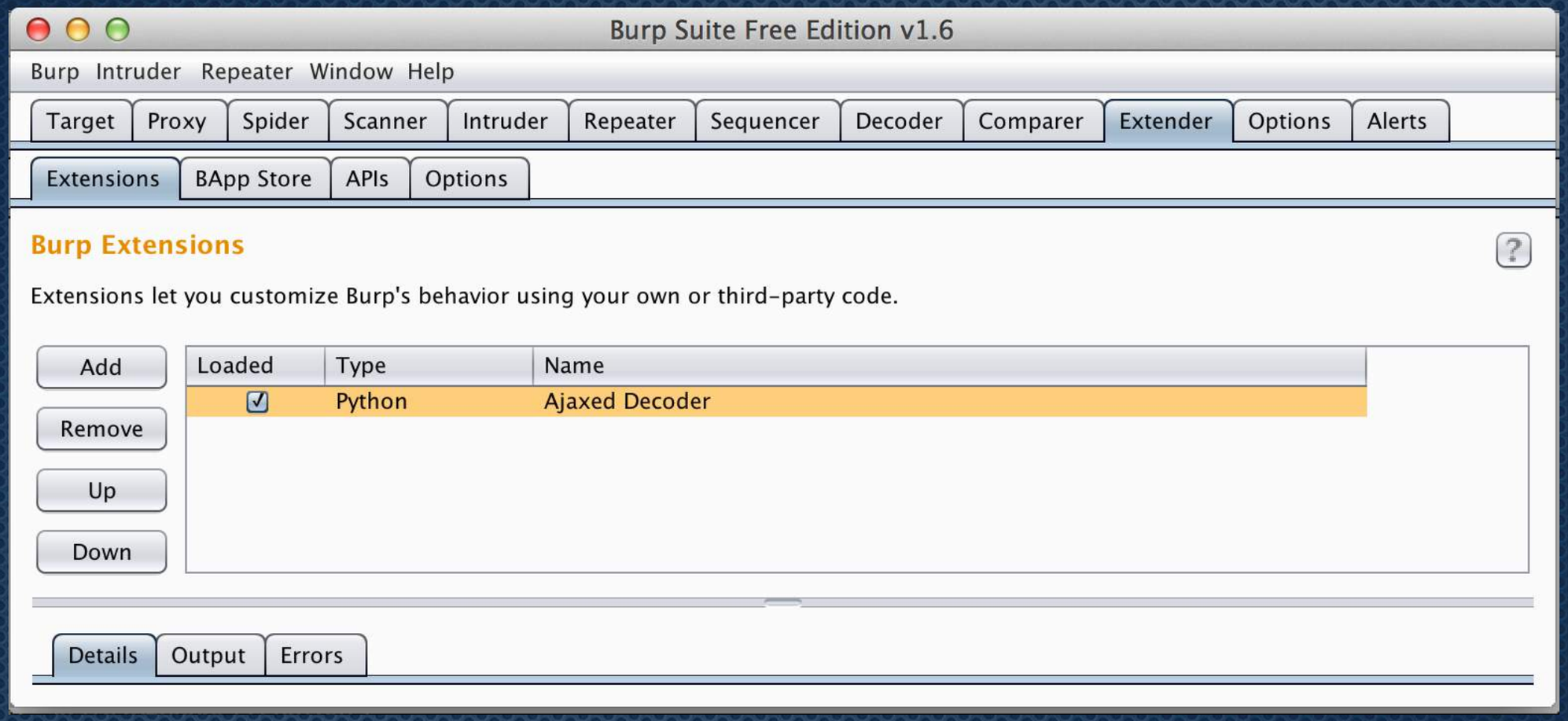
```
def isEnabled(self, content, isRequest):
  if isRequest:
    r = self._helpers.analyzeRequest(content)
  else:
    r = self._helpers.analyzeResponse(content)

  msg = content[r.getBodyOffset():].tostring()

  for header in r.getHeaders():
    if header.lower().startswith("content-type:"):
      content_type = header.split(":")[1].lower()
      if content_type.find("application/json") > 0:
        return True
      else:
        return False

  return False
```

Alive peoples

```
def setMessage(self, content, isRequest):
  if content is None:
    self._txtInput.setText(None)
    self._txtInput.setEditable(False)
  else:
    if isRequest:
      r = self._helpers.analyzeRequest(content)
    else:
      r = self._helpers.analyzeResponse(content)

    msg = content[r.getBodyOffset():].tostring()
    try:
      #Here place the decoder
      raise Exception()
    except:
      pretty_msg = msg

    self._txtInput.setText(pretty_msg)
    self._txtInput.setEditable(self._editable)

  self._currentMessage = content
  return
```

```
def getMessage(self):
  if self._txtInput.isTextModified():
    try:
      #Here place the encoder
      raise Exception()
    except Exception, e:
      data = self._helpers.bytesToString(self._txtInput.getText())

    # Reconstruct request/response
    r = self._helpers.analyzeRequest(self._currentMessage)

    return self._helpers.buildHttpMessage(r.getHeaders(), self._he
  else:
    return self._currentMessage
```

Setup the custom plugin



Challenge

- Go on “http://burp.pigbox.info”
- The GOAL is to have “Raciphalophatophane” as an user in members page with “admin” role.

This must be done by tamper the response with a burp plugin