New issue

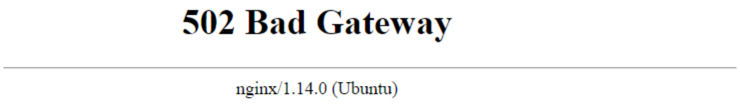
Jump to bottom

Unknow IP can let mhn web crash #799

⊙ Open FreddyMa1210 opened this issue on Nov 23, 2020 · 1 comment

FreddyMa1210 commented on Nov 23, 2020

At one day, my MHN Web page can not open but all service is well . So I try to find the reason and this is the reason as following.
If there is one IP address not in "GeoLite2-City.mmdb", then the ISO country code will return "None". When the code is "None", then the MHN Web can not generate icon path and the system will be crashed.



502 Bad Gateway

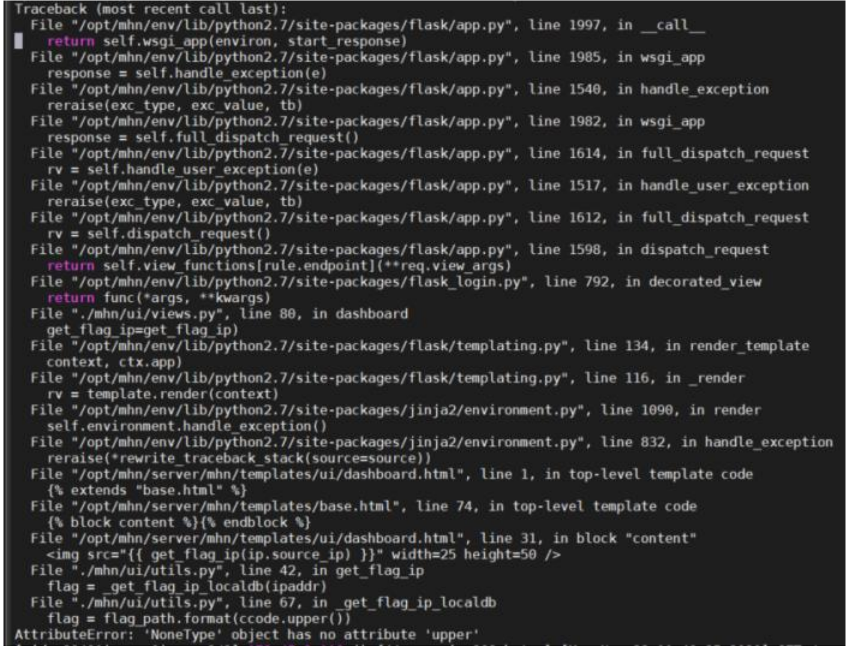
nginx/1.14.0 (Ubuntu)

Code: "mhn/server/mhn/ui/utils.py"

```
57  def _get_flag_ip_localdb(ipaddr):
58      flag_path = '/static/img/flags-iso/shiny/64/{}.png'
59      try:
60          r = geoip2_reader.city(ipaddr)
61          ccode = r.country.iso_code
62      except Exception:
63          app.logger.warning("Could not determine flag for ip (LOCALDB): {}".format(ipaddr))
64          return constants.DEFAULT_FLAG_URL
65      else:
66          # Constructs the flag source using country code
67          flag = flag_path.format(ccode.upper())
68          if os.path.exists(MHN_SERVER_HOME +"/mhn"+flag):
69              return flag
70          else:
71              return constants.DEFAULT_FLAG_URL
72
```

At function "_get_flag_ip_localdb" in line 61 if it work it can get IP ISO Code, but if IP has no record in "GeoLite2-City.mmdb" it will return None.
Next, line 67 can not use "upper function" to the IP ISO code. If the page need to show the country icon (Like Dashboard, Attack List...etc), then the page will be crashed.

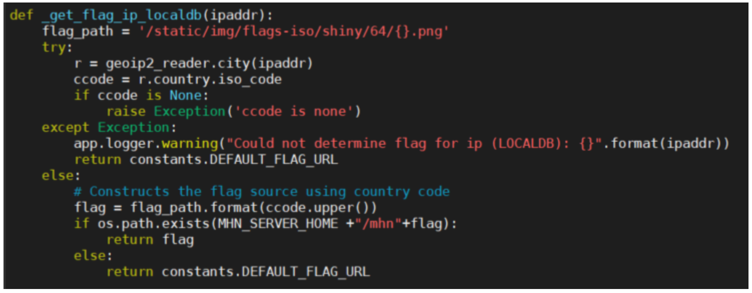
There is the crash log in "/var/log/mhn/mhn-uwsgi.err".



```
Traceback (most recent call last):
  File "/opt/mhn/env/lib/python2.7/site-packages/flask/app.py", line 1997, in __call__
    return self.wsgi_app(environ, start_response)
  File "/opt/mhn/env/lib/python2.7/site-packages/flask/app.py", line 1985, in wsgi_app
    response = self.handle_exception(e)
  File "/opt/mhn/env/lib/python2.7/site-packages/flask/app.py", line 1540, in handle_exception
    reraise(exc_type, exc_value, tb)
  File "/opt/mhn/env/lib/python2.7/site-packages/flask/app.py", line 1982, in wsgi_app
    response = self.full_dispatch_request()
  File "/opt/mhn/env/lib/python2.7/site-packages/flask/app.py", line 1614, in full_dispatch_request
    rv = self.handle_user_exception(e)
  File "/opt/mhn/env/lib/python2.7/site-packages/flask/app.py", line 1517, in handle_user_exception
    reraise(exc_type, exc_value, tb)
  File "/opt/mhn/env/lib/python2.7/site-packages/flask/app.py", line 1612, in full_dispatch_request
    rv = self.dispatch_request()
  File "/opt/mhn/env/lib/python2.7/site-packages/flask/app.py", line 1598, in dispatch_request
    return self.view_functions[rule.endpoint](**req.view_args)
  File "/opt/mhn/env/lib/python2.7/site-packages/flask_login.py", line 792, in decorated_view
    return func(*args, **kwargs)
  File "./mhn/ui/views.py", line 80, in dashboard
    get_flag_ip=get_flag_ip)
  File "/opt/mhn/env/lib/python2.7/site-packages/flask/templating.py", line 134, in render_template
    context, ctx.app)
  File "/opt/mhn/env/lib/python2.7/site-packages/flask/templating.py", line 116, in _render
    rv = template.render(context)
  File "/opt/mhn/env/lib/python2.7/site-packages/jinja2/environment.py", line 1090, in render
    self.environment.handle_exception()
  File "/opt/mhn/env/lib/python2.7/site-packages/jinja2/environment.py", line 832, in handle_exception
    reraise(*rewrite_traceback_stack(source=source))
  File "/opt/mhn/server/mhn/templates/ui/dashboard.html", line 1, in top-level template code
    {% extends "base.html" %}
  File "/opt/mhn/server/mhn/templates/base.html", line 74, in top-level template code
    {% block content %}{% endblock %}
  File "/opt/mhn/server/mhn/templates/ui/dashboard.html", line 31, in block "content"
    <img src="{{ get_flag_ip(ip.source_ip) }}" width=25 height=50 />
  File "./mhn/ui/utils.py", line 42, in get_flag_ip
    flag = _get_flag_ip_localdb(ipaddr)
  File "./mhn/ui/utils.py", line 67, in _get_flag_ip_localdb
    flag = flag_path.format(ccode.upper())
AttributeError: 'NoneType' object has no attribute 'upper'
```

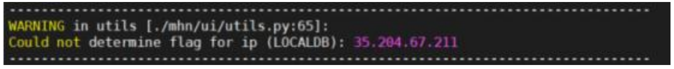
My case "IP 35[.]204[.]67[.]211" has no record in "GeoLite2-City.mmdb" (MD5: fd258548621120622e757631ef94f2cb).

So, I insert an "if" statement in "_get_flag_ip_localdb" to fix it.

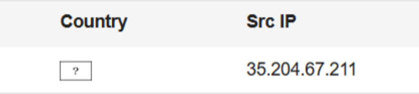


```python
def _get_flag_ip_localdb(ipaddr):
    flag_path = '/static/img/flags-iso/shiny/64/{}.png'
    try:
        r = geoip2_reader.city(ipaddr)
        ccode = r.country.iso_code
        if ccode is None:
            raise Exception('ccode is none')
    except Exception:
        app.logger.warning("Could not determine flag for ip (LOCALDB): {}".format(ipaddr))
        return constants.DEFAULT_FLAG_URL
    else:
        # Constructs the flag source using country code
        flag = flag_path.format(ccode.upper())
        if os.path.exists(MHN_SERVER_HOME +"/mhn"+flag):
            return flag
        else:
            return constants.DEFAULT_FLAG_URL
```

Now there will log the error in "/var/log/mhn/mhn-uwsgi.err" and page can show perfectly.



```
--------------------------------------------------------------------------------
WARNING in utils [./mhn/ui/utils.py:65]:
Could not determine flag for ip (LOCALDB): 35.204.67.211
--------------------------------------------------------------------------------
```



Country	Src IP
?	35.204.67.211

So if use a special IP address to connect honeypot, then it can do the "DoS attack" to MHN system.

NicoleG25 commented on Nov 30, 2020

Hi **@d1str0**, do you happen to know if this issue was ever addressed? please note that it was assigned CVE-2020-29069

Thanks in advance !

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants