Fixing a security vulnerability in http.cookiejar

Karthikeyan Singaravelan

- Backend developer at HappyFox.
- Core triager and contributor to CPython.
- Primarily interested in `unittest.mock` and security.
- GitHub : https://github.com/tirkarthi

Bugs happen!

- Bugs are reported at https://bugs.python.org. (Public)
- 48421 (closed - 41363, open - 7058) and counting.
- Security vulnerabilities should be reported to security@python.org (restricted access)

Cookie Jar

- An abstraction to store and send cookies while making http requests.
- Present in Chrome, Firefox, Python, Golang etc.
- Has a set of rules based on RFC 6265 to store and send cookies to relevant sites.

Incorrect domain check (issue35121)

- Lenient check using `endswith`

Original report

```
from http.cookiejar import DefaultCookiePolicy
from urllib.request import Request

policy = DefaultCookiePolicy()
req = Request('https://xxxfoo.co.jp/')
print(policy.domain_return_ok('foo.co.jp', req) # True
```

- Triaged it as a bug. Wrote a patch and left on the tracker for a month.

Analysis

- requests has `requests.session` that helps in handling cookies across requests. requests uses `http.cookiejar.DefaultCookiePolicy`

```
with requests.session() as session:
    session.get("https://example.com")
    # sends example.com cookies
    session.get("https://example.com")
    # sends example.com cookies too !!!
    session.get("https://badexample.com")
```

- Reported to requests team and was asked to patch it in CPython. Sent a report to security@python.org.
- Issue triaged as a security issue and release blocker.
- PR 1058. Reviewed and approved by Serhiy Storchaka and Alex Gaynor.

Incorrect path check (issue35647)

- Lenient check using `startswith`

```
with requests.session() as session:
    # Set a cookie with path=/any
    session.get("https://example.com/any")
    # Sends cookies
    session.get("https://example.com/any")
    # Sends cookies
    session.get("https://example.com/any/foo")
    # Sends cookies too !!!
    session.get("https://example.com/anybad/")
```

- Less severe since it's about path under same domain.
- PR 11436. Reviewed and approved by Senthil Kumaran and Alex Gaynor.

Backporting workflow

- Tests for the fix to ensure there are no regressions.
- Merged to master. Backported to 3.7, 3.6, 3.5 and 3.4.
- Python 2.7 awaiting the fix.
- Keep track of regressions for few releases.
- The code was from May 31, 2004 (Python 2.4).

Security and 2.7 EoL

- Since the bugs themselves are 15 years old. There could be more after 01/01/2020.
- There will always be new standards, attack vectors, RFCs, openssl, tls upgrades etc.
- No fixes to 2.7 after 2020.
- Please upgrade to Python 3.

Contribute to open source

- If your organization uses Python then please consider supporting the project by donating money or volunteer time.
- Contribution is not only about code. Testing, documenting, triaging and participating are also very important.
- Try looking into the tools you use daily
  - IPython (1141 open issues, 16 PRs)
  - Jupyter Notebook (1395 open issues, 63 PRs)
- Happy hacking :)