## Assignment

Given below are a couple of vendor vulnerability details websites. These sites contain the key vulnerability details we need to process.

https://www.mongodb.com/alerts
https://helpx.adobe.com/security/products/acrobat/apsb20-13.html

Your task is to write a program to parse the above sites and extract all key vulnerability metrics.Specifically, this information should be parsed and formatted into JSON content as defined by the given JSON schema.

Sample output for mongodb:


```
{
  "type": "vendor",
  "source": "mongodb",
   "cves": [
    {
      "timestamp": "2020-04-21T17:46Z",
      "published_date": "2019-08-31T05:00Z",
      "last_modified_date": "2019-11-01T19:11Z",
      "id": "CVE-2019-2390",
      "url": "https://www.mongodb.com/alerts",
      "name": "MongoDB Alerts",
      "description": "An unprivileged user or program defect.",
      "cpes": {
        "operator": "OR",
        "cpe_list": [
          {
            "vendor": "mongodb",
            "product": "mongodb",
            "category": "a",
            "versionStartIncluding": "4.0.0",
            "versionEndIncluding": "4.0.10"
          },
          {
            "vendor": "mongodb",
            "product": "mongodb",
            "category": "a",
            "versionStartIncluding": "3.6.0",
            "versionEndIncluding": "3.6.13"
          },
          {
            "vendor": "mongodb",
            "product": "mongodb",
            "category": "a",
            "versionStartIncluding": "3.4.0",
            "versionEndIncluding": "3.4.21"
          }
        ]
      }
    },
    {
      "timestamp": "2020-04-21T17:46Z",
      "published_date": "2014-06-17T00:00Z",
      "last_modified_date": "2015-10-29T04:26Z",
      "id": "CVE-2014-3971",
      "url": "https://www.mongodb.com/alerts",
      "name": "MongoDB Alerts",
      "description": "Remotely trigger a crash when X.509 is enabled",
      "cpes": {
        "operator": "OR",
        "cpe_list": [
          {
            "vendor": "mongodb",
            "product": "mongodb",
            "category": "a",
            "version": "2.6.0"
          },
          {
            "vendor": "mongodb",
```

```
            "product": "mongodb",
            "category": "a",
            "version": "2.6.1"
          }
        ]
      }
    }
  ]
}
```


Sample output for adobe experience-manager:


```
{
    "source": "adobe",
    "type": "vendor",
    "cves": [
        {
            "timestamp": "2020-03-12T18:06Z",
            "published_date": "2020-01-14T00:00Z",
            "id": "CVE-2019-16466",
            "url": "https://helpx.adobe.com/security/products/experience-manager/
apsb20-01.html",
            "name": "APSB20-01 Security update available for Adobe Experience Manager",
            "description": "cross-site script inclusion",
            "cpes": {
                "operator": "OR",
                "cpe_list": [
                    {
                        "vendor": "adobe",
                        "product": "experience_manager",
                        "category": "a",
                        "versionStartIncluding": "6.0",
                        "versionEndIncluding": "6.5",
                        "cpe23Uri": "cpe:2.3:a:adobe:experience_manager:*:*:*:*:*:*:*:*"
                    }
                ]
            },
            "cvssv2": {
                "severity": "HIGH"
            },
            "cvssv3": {
                "severity": "HIGH"
            }
        },
        {
            "timestamp": "2020-03-12T18:06Z",
            "published_date": "2020-01-14T00:00Z",
            "id": "CVE-2019-16467",
            "url": "https://helpx.adobe.com/security/products/experience-manager/
apsb20-01.html",
            "name": "APSB20-01 Security update available for Adobe Experience Manager",
            "description": "reflected cross-site scripting",
            "cpes": {
                "operator": "OR",
                "cpe_list": [
                    {
                        "vendor": "adobe",
                        "product": "experience_manager",
                        "category": "a",
                        "versionStartIncluding": "6.0",
                        "versionEndIncluding": "6.5",
                        "cpe23Uri": "cpe:2.3:a:adobe:experience_manager:*:*:*:*:*:*:*:*"
                    }
                ]
            },
            "cvssv2": {
                "severity": "HIGH"
            },
            "cvssv3": {
                "severity": "HIGH"
            }
        },
        {
            "timestamp": "2020-03-12T18:06Z",
            "published_date": "2020-01-14T00:00Z",
```

```
            "id": "CVE-2019-16468",
            "url": "https://helpx.adobe.com/security/products/experience-manager/
apsb20-01.html",
            "name": "APSB20-01 Security update available for Adobe Experience Manager",
            "description": "user interface injection",
            "cpes": {
                "operator": "OR",
                "cpe_list": [
                    {
                        "vendor": "adobe",
                        "product": "experience_manager",
                        "category": "a",
                        "versionStartIncluding": "6.0",
                        "versionEndIncluding": "6.5",
                        "cpe23Uri": "cpe:2.3:a:adobe:experience_manager:*:*:*:*:*:*:*:*"
                    }
                ]
            },
            "cvssv2": {
                "severity": "MEDIUM"
            },
            "cvssv3": {
                "severity": "MEDIUM"
            }
        },
        {
            "timestamp": "2020-03-12T18:06Z",
            "published_date": "2020-01-14T00:00Z",
            "id": "CVE-2019-16469",
            "url": "https://helpx.adobe.com/security/products/experience-manager/
apsb20-01.html",
            "name": "APSB20-01 Security update available for Adobe Experience Manager",
            "description": "expression language injection",
            "cpes": {
                "operator": "OR",
                "cpe_list": [
                    {
                        "vendor": "adobe",
                        "product": "experience_manager",
                        "category": "a",
                        "versionStartIncluding": "6.0",
                        "versionEndIncluding": "6.5",
                        "cpe23Uri": "cpe:2.3:a:adobe:experience_manager:*:*:*:*:*:*:*:*"
                    }
                ]
            },
            "cvssv2": {
                "severity": "HIGH"
            },
            "cvssv3": {
                "severity": "HIGH"
            }
        }
    ]
}
```


JSON schema

```
{
  'source': <vendor name>,
  'type': 'vendor',
  'cves': [
    {
      'timestamp': <current time>,
      'published_date': <Published date from page, empty (if unavailable)
      'last_modified_date': <Updated date from page, empty (if unavailable),
       'id': <CVE ID>,
      'url': <Source URL>,
      'name': <source name / title>,
      'description': <CVE description>,
      'cpes': {
        'operator': 'OR',
        'cpe_list': [
          {
            'vendor': <vendor name>,
```

```
            'product': <product name>,
            'category': 'a',
            'version': <version string>, (only for single version)
            'versionStartIncluding': <version string>, (for version range)
            'versionStartExcluding': <version string>, (for version range)
            'versionEndIncluding': <version string>, (for version range)
            'versionEndExcluding': <version string>,(for version range)
            'update': <update string, omitted if not available>,
            'sw_edition': <sw_edition string, omitted if not available>,
            'patches': [
              <patch ID string, omitted if not available>
            ],
            'cpe23Uri': <cpe if available, omitted otherwise>
          }
        ]
      },
      'cvssv2': {
        'vector_string': <if available, else None>,
        'base_score': <if available, else None>,
        'severity': <if available, else None>
      },
      'cvssv3': {
        'vector_string': <if available, else None>,
        'base_score': <if available, else None>,
        'severity': <if available, else None>
      },
      'patches': [
        {
          'patch_id': <patch number string>,
          'reference': <patch url>,
          'supersedes': [<patch_id>],
          'restart_needed': <True, False, None>,
          'patch_type': <type string>,
          'release_date': <Patch release date>
        }
      ]
    }
  ]
}
```

## Instructions and requirements

- Your code should take a website URL as input and output a file with JSON formatted CVE information as given in the sample
- It should work seamlessly on websites that have content/layout similar to the example sites provided above
- Code should be written in Python3, please make sure to follow python coding standards
    - https://docs.python-guide.org/writing/style/
- Code, scripts and documentation (if any) should be packaged as .zip or .tar archive
- Add any instructions in a README that will help run the code on any machine
- Log enough information in case of errors to troubleshoot the error
- Make sure to test your code well before submitting
- Your code will be subjected to a quality check that includes manual review, automated tests against an existing test suite and manual testing.