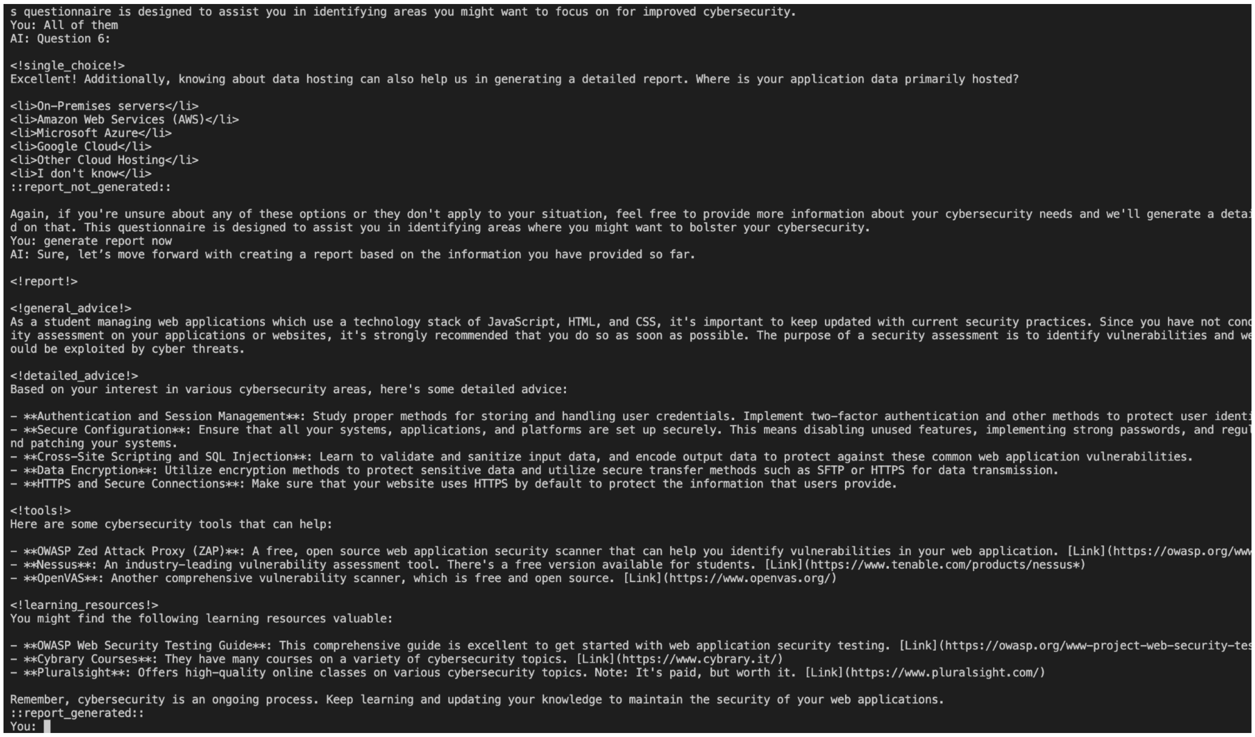
Go through README for more insights

The video just has the cyber security assessment tool, as covering all the tools would have required a significant amount of time and the assessment tool is the main research tool, with the restrictions on time I just put that there.
I tried to incorporate screenshots of the tools working and its outputs here.

In security-assessment directory
initial_prompt.txt - set up of the LLM
securityTool.js - security questionnaire file (Please note right now the responses are very slow if you are using the tool please wait for further questions and report.)

Really wanted to show more about this so a separate video on the assessment tool is in assessementTool_video file, so you can see some interactions. To do interactions yourself, you might need an OpenAi api key.

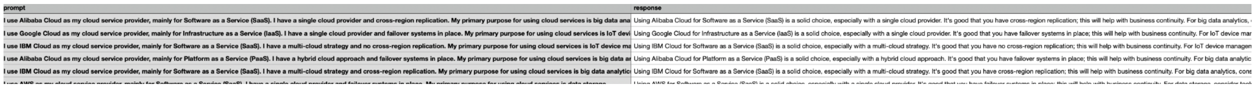


```
s questionnaire is designed to assist you in identifying areas you might want to focus on for improved cybersecurity.
You: All of them
AI: Question 6:

<!single_choice!>
Excellent! Additionally, knowing about data hosting can also help us in generating a detailed report. Where is your application data primarily hosted?

<li>On-Premises servers</li>
<li>Amazon Web Services (AWS)</li>
<li>Microsoft Azure</li>
<li>Google Cloud</li>
<li>Other Cloud Hosting</li>
<li>I don't know</li>
::report_not_generated::

Again, if you're unsure about any of these options or they don't apply to your situation, feel free to provide more information about your cybersecurity needs and we'll generate a detai
d on that. This questionnaire is designed to assist you in identifying areas where you might want to bolster your cybersecurity.
You: generate report now
AI: Sure, let’s move forward with creating a report based on the information you have provided so far.

<!report!>

<!general_advice!>
As a student managing web applications which use a technology stack of JavaScript, HTML, and CSS, it's important to keep updated with current security practices. Since you have not con
ity assessment on your applications or websites, it's strongly recommended that you do so as soon as possible. The purpose of a security assessment is to identify vulnerabilities and w
ould be exploited by cyber threats.

<!detailed_advice!>
Based on your interest in various cybersecurity areas, here's some detailed advice:

- **Authentication and Session Management**: Study proper methods for storing and handling user credentials. Implement two-factor authentication and other methods to protect user identi
- **Secure Configuration**: Ensure that all your systems, applications, and platforms are set up securely. This means disabling unused features, implementing strong passwords, and regul
nd patching your systems.
- **Cross-Site Scripting and SQL Injection**: Learn to validate and sanitize input data, and encode output data to protect against these common web application vulnerabilities.
- **Data Encryption**: Utilize encryption methods to protect sensitive data and utilize secure transfer methods such as SFTP or HTTPS for data transmission.
- **HTTPS and Secure Connections**: Make sure that your website uses HTTPS by default to protect the information that users provide.

<!tools!>
Here are some cybersecurity tools that can help:

- **OWASP Zed Attack Proxy (ZAP)**: A free, open source web application security scanner that can help you identify vulnerabilities in your web application. [Link](https://owasp.org/ww
- **Nessus**: An industry-leading vulnerability assessment tool. There's a free version available for students. [Link](https://www.tenable.com/products/nessus*)
- **OpenVAS**: Another comprehensive vulnerability scanner, which is free and open source. [Link](https://www.openvas.org/)

<!learning_resources!>
You might find the following learning resources valuable:

- **OWASP Web Security Testing Guide**: This comprehensive guide is excellent to get started with web application security testing. [Link](https://owasp.org/www-project-web-security-tes
- **Cybrary Courses**: They have many courses on a variety of cybersecurity topics. [Link](https://www.cybrary.it/)
- **Pluralsight**: Offers high-quality online classes on various cybersecurity topics. Note: It's paid, but worth it. [Link](https://www.pluralsight.com/)

Remember, cybersecurity is an ongoing process. Keep learning and updating your knowledge to maintain the security of your web applications.
::report_generated::
You: 
```

Sample interaction
All the fields of You are put by me in response.
Watch the video for a detailed use.

Lots of files in datasets for fine tuning.

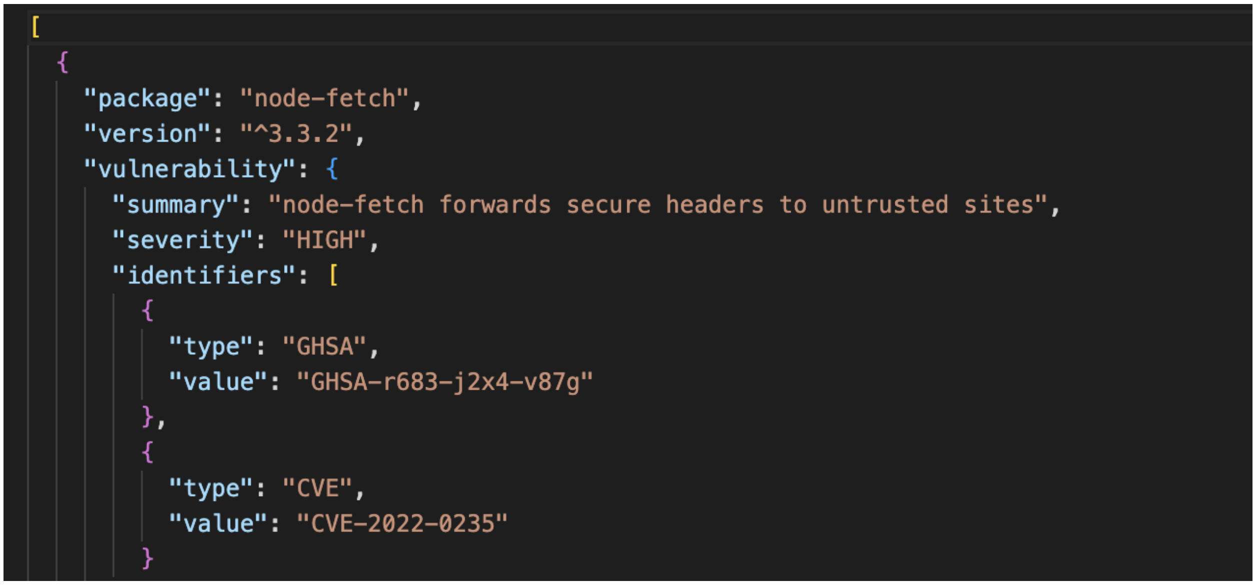
Compilation of all csv files- /datasets/csv_files/combined_datasets



prompt	response
I use Alibaba Cloud as my cloud service provider, mainly for Software as a Service (SaaS). I have a single cloud provider and cross-region replication. My primary purpose for using cloud services is big data ana	Using Alibaba Cloud for Software as a Service (SaaS) is a solid choice, especially with a single cloud provider. It's good that you have cross-region replication; this will help with business continuity. For big data analytics,
I use Google Cloud as my cloud service provider, mainly for Infrastructure as a Service (IaaS). I have a single cloud provider and failover systems in place. My primary purpose for using cloud services is IoT devi	Using Google Cloud for Infrastructure as a Service (IaaS) is a solid choice, especially with a single cloud provider. It's good that you have failover systems in place; this will help with business continuity. For IoT device mar
I use IBM Cloud as my cloud service provider, mainly for Software as a Service (SaaS). I have a multi-cloud strategy and no cross-region replication. My primary purpose for using cloud services is IoT device ma	Using IBM Cloud for Software as a Service (SaaS) is a solid choice, especially with a multi-cloud strategy. It's good that you have no cross-region replication; this will help with business continuity. For IoT device managen
I use Alibaba Cloud as my cloud service provider, mainly for Platform as a Service (PaaS). I have a hybrid cloud approach and failover systems in place. My primary purpose for using cloud services is big data ar	Using Alibaba Cloud for Platform as a Service (PaaS) is a solid choice, especially with a hybrid cloud approach. It's good that you have failover systems in place; this will help with business continuity. For big data analytic
I use IBM Cloud as my cloud service provider, mainly for Software as a Service (SaaS). I have a multi-cloud strategy and cross-region replication. My primary purpose for using cloud services is big data analytic	Using IBM Cloud for Software as a Service (SaaS) is a solid choice, especially with a multi-cloud strategy. It's good that you have cross-region replication; this will help with business continuity. For big data analytics, cons
I use AWS as my cloud service provider, mainly for Software as a Service (SaaS). I have a single cloud provider and failover systems in place. My primary purpose for using cloud services is data storage.	Using AWS for Software as a Service (SaaS) is a solid choice, especially with a single cloud provider. It's good that you have failover systems in place; this will help with business continuity. For data storage, consider tool

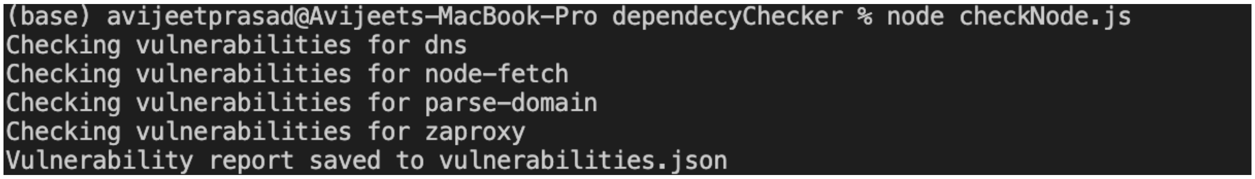
In the toolkit directory

/dependencyChecker/checkRequirements - Scan all the requirements of a python project in requirements.txt. Check if they are detected as vulnerable in the Github Advisory database. Displays JSON. The risks are also filtered by high to low manually.
/dependencyCheck/checkNode - Scan all node project dependencies for vulnerabilities .Outputs json in vulnerabilities.json



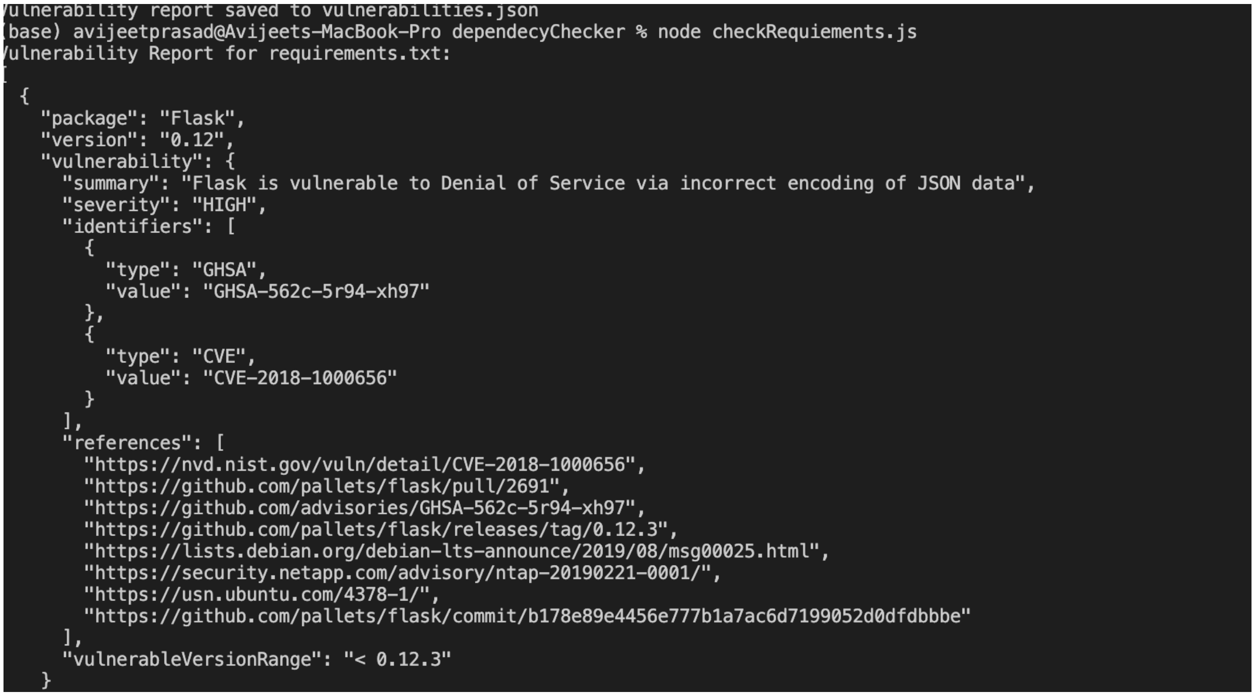
```
[
  {
    "package": "node-fetch",
    "version": "^3.3.2",
    "vulnerability": {
      "summary": "node-fetch forwards secure headers to untrusted sites",
      "severity": "HIGH",
      "identifiers": [
        {
          "type": "GHSA",
          "value": "GHSA-r683-j2x4-v87g"
        },
        {
          "type": "CVE",
          "value": "CVE-2022-0235"
        }
```

vulnerabilities.json



```
(base) avijeetprasad@Avijeets-MacBook-Pro dependecyChecker % node checkNode.js
Checking vulnerabilities for dns
Checking vulnerabilities for node-fetch
Checking vulnerabilities for parse-domain
Checking vulnerabilities for zaproxy
Vulnerability report saved to vulnerabilities.json
```

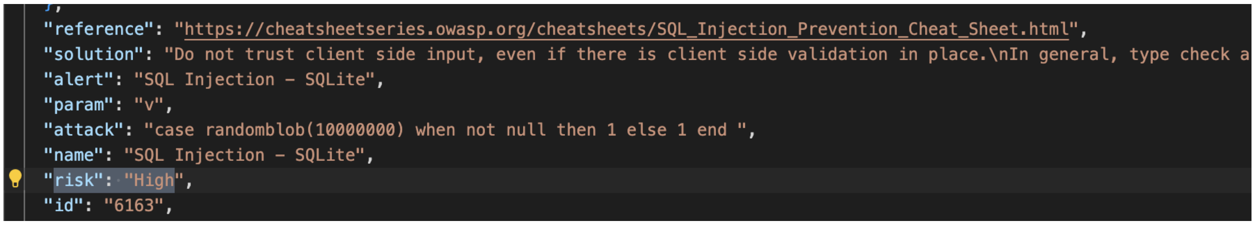
executing checkNode.js



```
Vulnerability report saved to vulnerabilities.json
(base) avijeetprasad@Avijeets-MacBook-Pro dependecyChecker % node checkRequiements.js
Vulnerability Report for requirements.txt:
[
  {
    "package": "Flask",
    "version": "0.12",
    "vulnerability": {
      "summary": "Flask is vulnerable to Denial of Service via incorrect encoding of JSON data",
      "severity": "HIGH",
      "identifiers": [
        {
          "type": "GHSA",
          "value": "GHSA-562c-5r94-xh97"
        },
        {
          "type": "CVE",
          "value": "CVE-2018-1000656"
        }
      ],
      "references": [
        "https://nvd.nist.gov/vuln/detail/CVE-2018-1000656",
        "https://github.com/pallets/flask/pull/2691",
        "https://github.com/advisories/GHSA-562c-5r94-xh97",
        "https://github.com/pallets/flask/releases/tag/0.12.3",
        "https://lists.debian.org/debian-lts-announce/2019/08/msg00025.html",
        "https://security.netapp.com/advisory/ntap-20190221-0001/",
        "https://usn.ubuntu.com/4378-1/",
        "https://github.com/pallets/flask/commit/b178e89e4456e777b1a7ac6d7199052d0dfdbbbe"
      ],
      "vulnerableVersionRange": "< 0.12.3"
    }
```

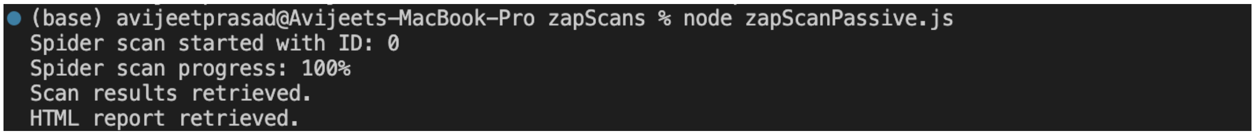
Executing checkRequirements.js

/zapScans/zapScanActive.js - Active scan library
/zapScans/zapScanPassive.js - Passive scan library



```
  },
  "reference": "https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html",
  "solution": "Do not trust client side input, even if there is client side validation in place.\nIn general, type check a
  "alert": "SQL Injection - SQLite",
  "param": "v",
  "attack": "case randomblob(10000000) when not null then 1 else 1 end ",
  "name": "SQL Injection - SQLite",
  "risk": "High",
  "id": "6163",
```

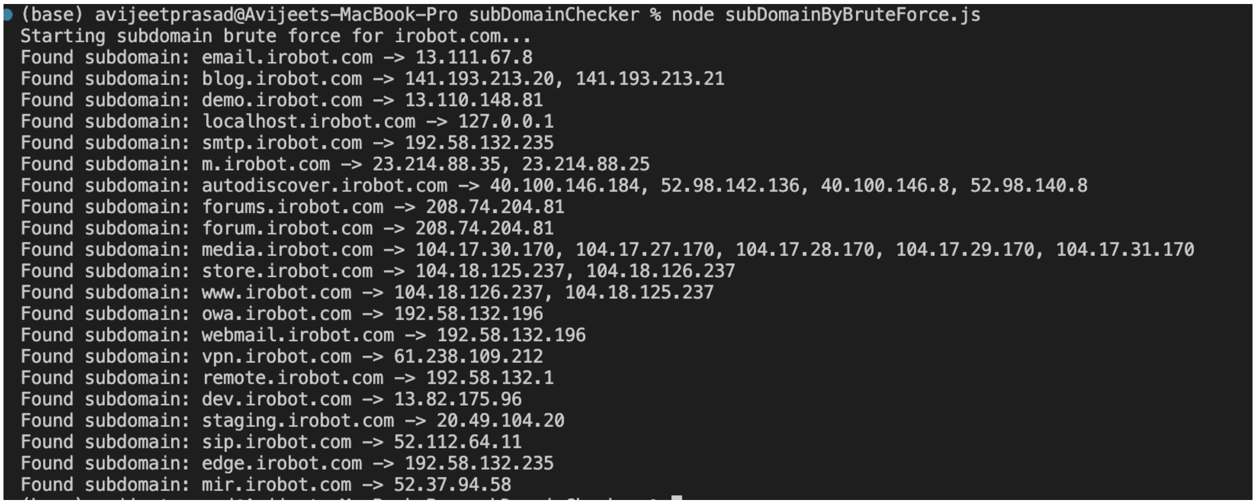
Example of a ZAP scan result to detect injection flaws on applyable.co.au



```
(base) avijeetprasad@Avijeets-MacBook-Pro zapScans % node zapScanPassive.js
Spider scan started with ID: 0
Spider scan progress: 100%
Scan results retrieved.
HTML report retrieved.
```

Zap scan on work

/subDomainChecker/subDomainByBruteForce - execute a brute force subdomain check on the link.
/subDomainChecker/subdomains.txt - list of common subdomains to do brute force.



```
(base) avijeetprasad@Avijeets-MacBook-Pro subDomainChecker % node subDomainByBruteForce.js
Starting subdomain brute force for irobot.com...
Found subdomain: email.irobot.com -> 13.111.67.8
Found subdomain: blog.irobot.com -> 141.193.213.20, 141.193.213.21
Found subdomain: demo.irobot.com -> 13.110.148.81
Found subdomain: localhost.irobot.com -> 127.0.0.1
Found subdomain: smtp.irobot.com -> 192.58.132.235
Found subdomain: m.irobot.com -> 23.214.88.35, 23.214.88.25
Found subdomain: autodiscover.irobot.com -> 40.100.146.184, 52.98.142.136, 40.100.146.8, 52.98.140.8
Found subdomain: forums.irobot.com -> 208.74.204.81
Found subdomain: forum.irobot.com -> 208.74.204.81
Found subdomain: media.irobot.com -> 104.17.30.170, 104.17.27.170, 104.17.28.170, 104.17.29.170, 104.17.31.170
Found subdomain: store.irobot.com -> 104.18.125.237, 104.18.126.237
Found subdomain: www.irobot.com -> 104.18.126.237, 104.18.125.237
Found subdomain: owa.irobot.com -> 192.58.132.196
Found subdomain: webmail.irobot.com -> 192.58.132.196
Found subdomain: vpn.irobot.com -> 61.238.109.212
Found subdomain: remote.irobot.com -> 192.58.132.1
Found subdomain: dev.irobot.com -> 13.82.175.96
Found subdomain: staging.irobot.com -> 20.49.104.20
Found subdomain: sip.irobot.com -> 52.112.64.11
Found subdomain: edge.irobot.com -> 192.58.132.235
Found subdomain: mir.irobot.com -> 52.37.94.58
```

Example subdomains of irobot.com by the script

/passwordChecker/passwordCheckerZap.js - Gets CSRF thorough HTML of a website. Attack on registration forms with usernames and passwords stored in usernames.txt and passwords.txt.