jscodeaudit.com

ACME.COM/SHOP

11th June, 2021

Abstract

This document provides a high-level overview of the most important problems in the acme.com/shop project.

We split these problems into two categories:

- Urgent: needs to be addressed, hardcoded passwords, SQL injection and other, similar exploits
- Other: instances that could improve the overall quality of the codebase, and make development experience better

Conclusion

Urgent

Problems that need to be addresses immediately:

SQL injections

https://github.com/akoskm/akoskm.github.io/blob/master/assets/js/prism.js#L5

https://github.com/akoskm/akoskm.github.io/blob/master/assets/js/prism.js#L9

...

Should be relatively easy to fix by using postgresql clients built-in positional arguments.

SQL User

Database connectivity is established through the postgres account. This means the attacker will have complete access to the entire database - not just the middlayer db.

Hardcoded passwords

https://github.com/akoskm/akoskm.github.io/blob/master/assets/js/prism.js#L11

These should be replaced with environment variables and should be supplied when starting the service in production.

Other

CORS

Requests are allowed from any domain:

```
res.header("Access-Control-Allow-Origin", "*");
```

https://github.com/akoskm/akoskm.github.io/blob/master/assets/js/prism.js#L1