OWASP Top 10

owasp.org

A10 Unvalidated Redirects and Forwards

A10 Unvalidated Redirects and Forwards

- OAuth
- Phishing attacks
- Firewall bypass

A9 Using Components with Known Vulnerabilities

A9 Using Components with Known Vulnerabilities

- roave/security-advisories
- nodesecurity.io
- retire.js

A8 Cross Site Request Forgery

A8 Cross Site Request Forgery

- `csrf_protection`
- `SameSite=strict`
- XSS always enables CSRF

A7 Missing Function Level Access Control

A7 Missing Function Level Access Control

- `web/`
- `app_dev.php` protection
- CSRF
- `is_granted`
- `@Secure`
- Whitelists

A6 Sensitive Data Exposure

A6 Sensitive Data Exposure

- TLS 1.2
- AES 128
- SHA 265
- HSTS
- Secret Valut
- Errors & Stack traces

A5 Security Misconfiguration

A5 Security Misconfiguration

- `allow_url_fopen`
- `allow_url_include`
- Billion laughs attack
- Backups
- `display_errors`
- Insecure defaults

A4 Insecure Direct Object References

A4 Insecure Direct Object References

Broken Access Control

- `require $_GET['page']`
- `is_granted`
- `@Secure`
- Use indirect access

A3 XSS

A3 XSS

- Autoescaping
- `dangerouslySetInnerHTML`
- `Content-type`
- Content-Security-Policy
- HTMLPurifier
- Whitelisting

A2 Weak authentication and session management

A2 Weak authentication and session management

- `httpOnly` and `secure` cookies
- CSRF tokens
- Firewall
- hashing secrets & tokens
- Session timeouts
- Brute force attacks

A1 Injection

A1 Injection

- ORM
- Prepared Statements
- QueryBuilder
- `{{ … | raw }}`
- `json_encode`
- `escapeshellarg`
- ProcessBuilder
- `mail()`

sammy is my hero