SECURITY AND YOUR VAPOR APPLICATION

TIM CONDON

BBC
Broken Hands

INTRODUCTION

- Varied background, currently at the BBC
- @0xTim - Twitter/Slack/Github
- @brokenhandsio - Twitter/Github
- Created SteamPress, Vapor Security Headers, Vapor OAuth

AGENDA

- Passwords
- HTTPS
- CSP
- Leaf
- Cookies
- CSRF
- Input Sanitation
- Server Configuration

CAVEATS!

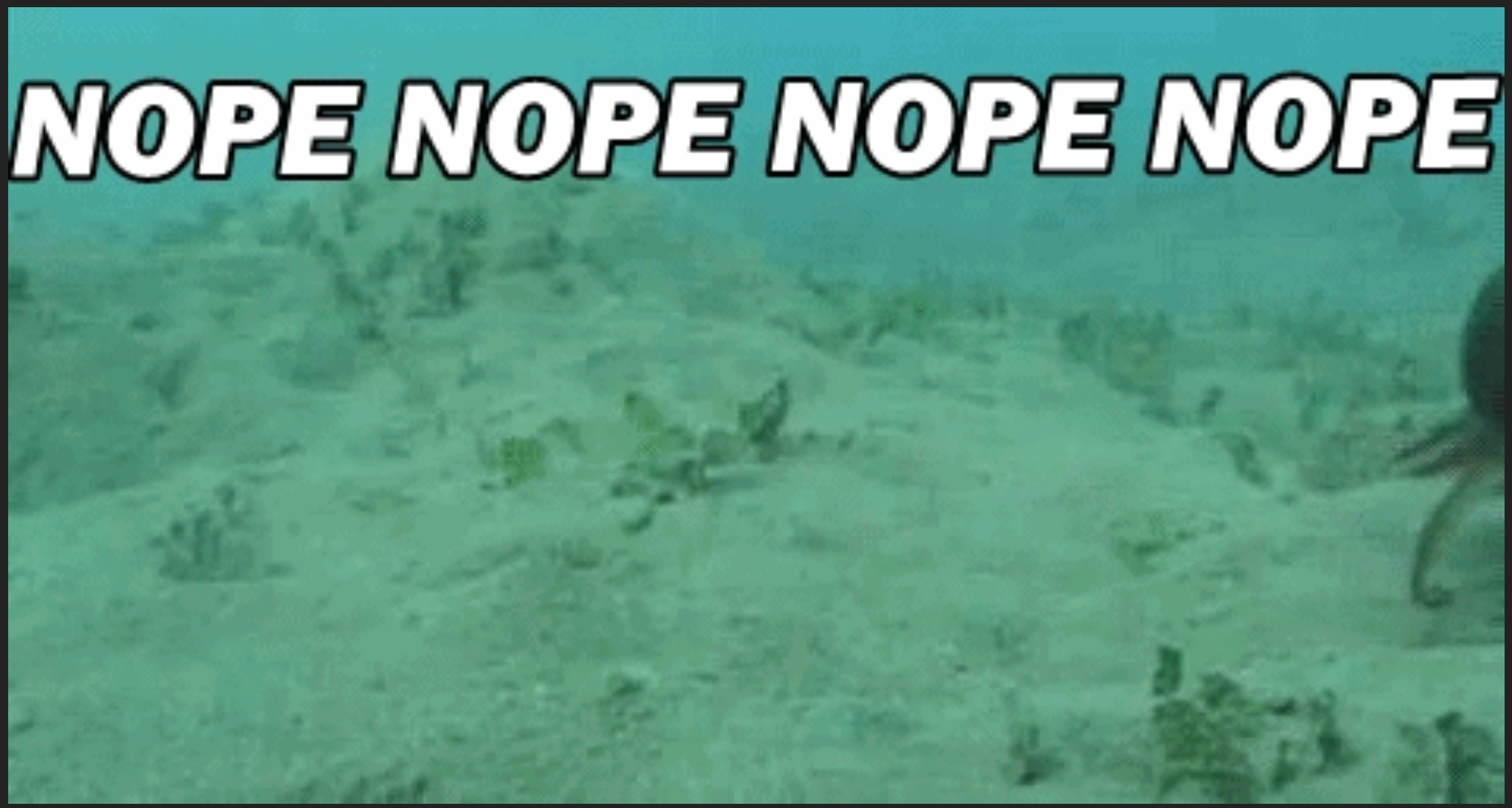
- No system is ever 100% secure
- Know your threat vector and attackers
- Security is like an onion - layers!

PASSWORDS

PASSWORDS

- Should I try and implement my own strategy?

PASSWORDS



PASSWORDS

- Use BCrypt

PASSWORDS

- PBKDF2 is an alternative - only if you've heard of it
- Do not save the password anywhere before hashing
- It should not be logged anywhere
- If you can email your user their password then you have a problem
- Do not give hints when logging in
- Resetting a password should be a token sent externally

AUTHENTICATION VS AUTHORISATION

- Authentication is verifying who someone is (e.g. logging in)
- Authorisation is verifying that user is allowed to do what they want
- Think about your authorisation flows and test them
- Require password to destructive options
- Do NOT do authentication or authorisation via queries or cookies!
- Logins should be rate limited

HTTPS

HTTPS

- No excuse!
- Secures communication between your user and your server
- Stops content injection
- Pins certificates where possible
- HSTS/OCSP Stapling/CAA/CT

HSTS

- HTTP Strict Transport Security
- Set as a header
- Ensures your site is HTTPS
- Preload with browsers to prevent the initial request being downgraded
- WARNING - must ensure all future traffic on all domains is HTTPS

CERTIFICATE PINNING

- Ensure that the HTTPS certificate being presented is one you know about
- Good for mobile
- HPKP is now on it’s way out on the web mainly due to HPKP suicide

OCSP STAPLING CAA AND CT

- CAA (Certificate Authority Authorisation) ensures that only allowed CAs can issue certificates
- Certificate Transparency allows you to monitor issued certificates
- Revoking certificates is hard
- OCSP (Online Certificate Status Protocol) Staples ensure that certificates are valid
- Can be enforced with Expect-Staple header

CSP

CONTENT SECURITY POLICY

- One of the quickest wins for security
- Prevents XSS attacks, downgrades attacks, insecure loading
- Set which domains scripts/images/stylesheets can be loaded from
- Do not allow eval or unsafe-inline
- Use SRI
- Use upgrade-insecure-requests

LEAF

LEAF

- No templating languages are secure - they have all been hacked
- Program defensively
- Only pass what you need
- Do NOT pass the request
- Do NOT pass the user's password - should only be set in the `makeRow()` function

CSRF

CROSS SITE REQUEST FORGERY

- An attacker makes a user submit a form e.g. transfer money
- Protect with token (and/or cookies)
- Package in Vapor Community
- Easy to implement otherwise

COOKIES

COOKIES

- Contain lots of valuable information
- Usual target for attacks
- Javascript should not be able to access them
- Mark them as secure

SECURE COOKIES

- Draft support for Same Site - protects against CSRF
- Implemented in Vapor - either use Lax or multi-cookies with Strict
- Cookie Prefixes enforce correct use of Secure and ensure that domain matches and the path is correct

INPUT SANITATION

INPUT SANITATION

- Don’t trust the client
- Careful with database calls (you have to try on Vapor)
- Ensure you validate all inputs server-side
- Be careful with parsing libraries
- IDs shouldn’t really be incrementing integers

SERVER CONFIGURATION

SERVER CONFIGURATION

- Don’t touch sudo
- Only expose the ports and services you need - don’t expose SSH to the world
- Check default password
- Check S3 buckets
- Check databases
- Updates!
- Don’t announce versions or server applications

TIM.CONDON@BBC.CO.UK

WE'RE HIRING!

USEFUL LINKS

- www.owasp.org
- www.securityheaders.io
- github.com/brokenhandsio/VaporSecurityHeaders

QUESTIONS