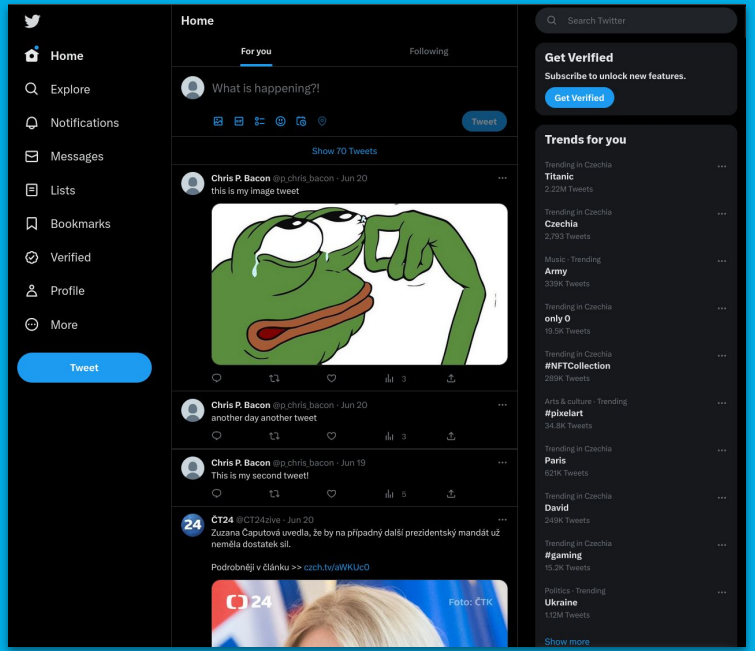
Twitter

BI-EHA.21 Semestral work

Jan Koníř, Tadeáš Kouba

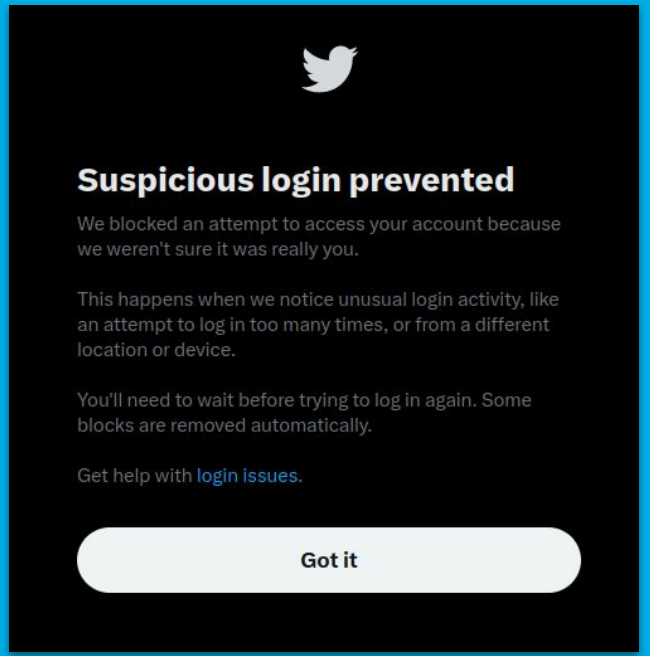
What is Twitter?

- Online social networking platform
- Mobile and Web application
- Tweets, retweets and reactions
- Direct messages
- Followers
- Timeline and Trends



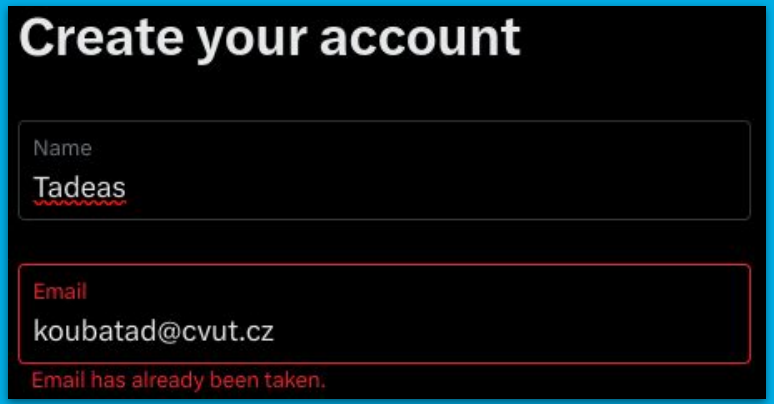
Account Lockout

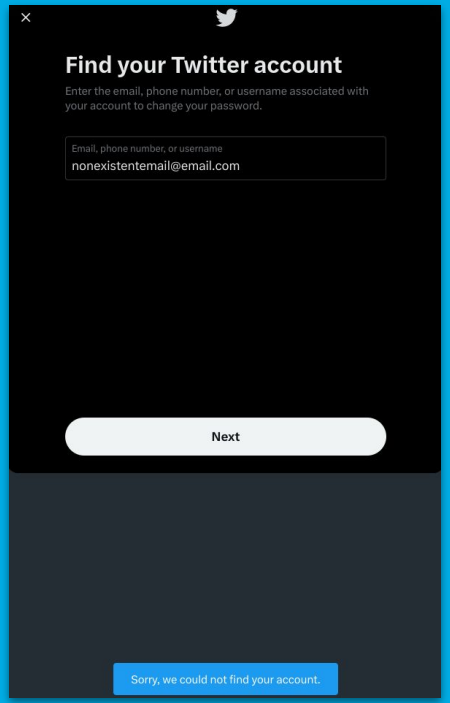
- CVSS 6.5 (Medium)
- Possibility to lock-out legitimate user
- Happens after 5-15 unsuccessful tries
- Takes 30+ minutes



User Enumeration

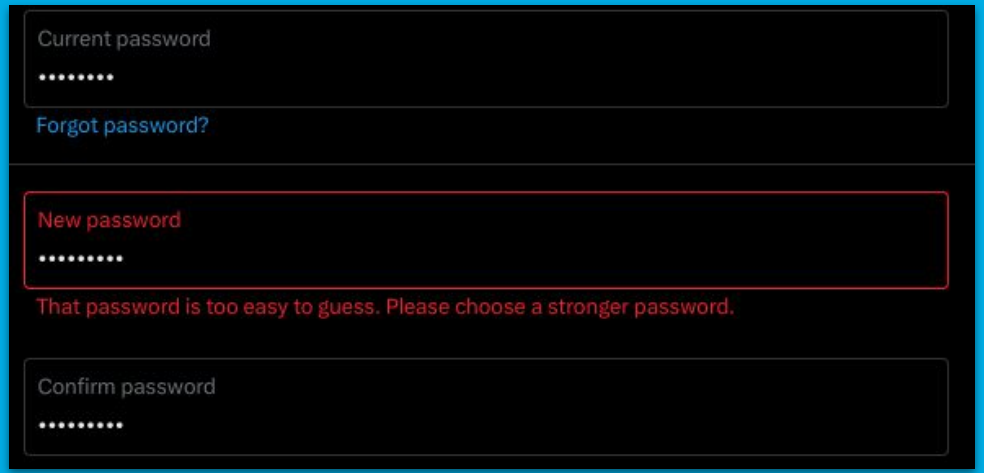
- CVSS 5.3 (Medium)
- Possibility to disclose user emails
- Login, Registration and Forgot password page





Password Check Inconsistent

- CVSS 0.0 (None)
- Different password checks performed
- Registration x Change password
- When registering user does not have username yet



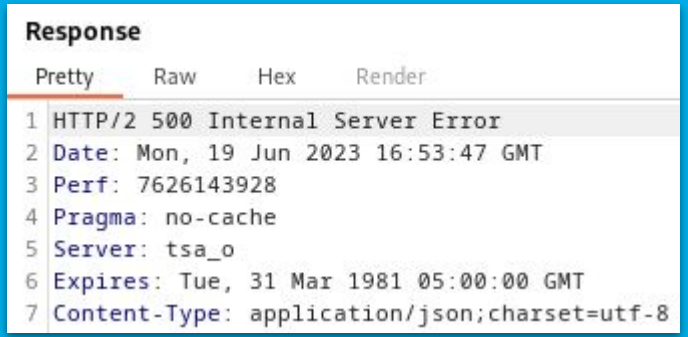
Missing HSTS Directive

- CVSS 0.0 (None)
- HTTP messages from the server are missing the *includeSubDomain* directive of HTTP Secure Transport Security header

```
Strict-Transport-Security: max-age=631138519
Cross-Origin-Opener-Policy: same-origin-allow-popups
Cross-Origin-Embedder-Policy: unsafe-none
X-Response-Time: 121
```

Internal Server Error

- CVSS 0.0 (None)
- Invalid JSON object caused the server to respond with 500 Internal Server Error



Thank you for your attention

Any questions?