

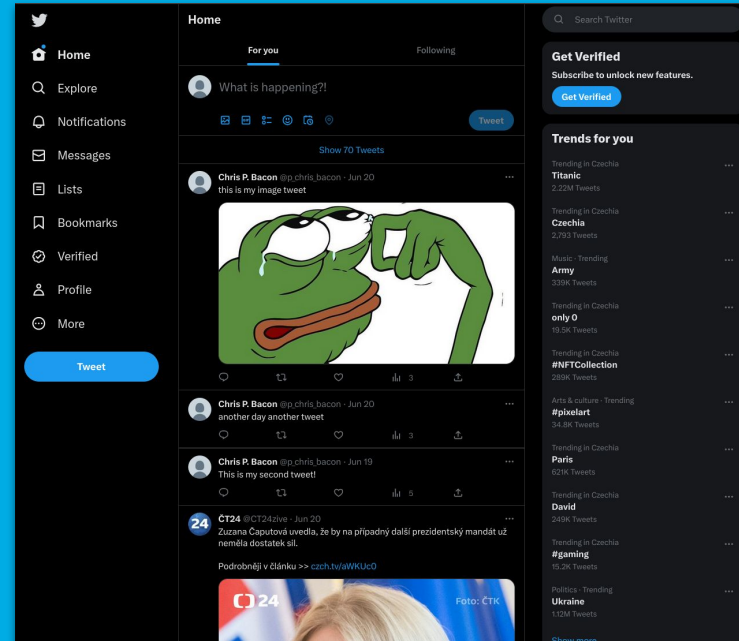


# Twitter

BI-EHA.21 Semestral work  
Jan Koníř, Tadeáš Kouba

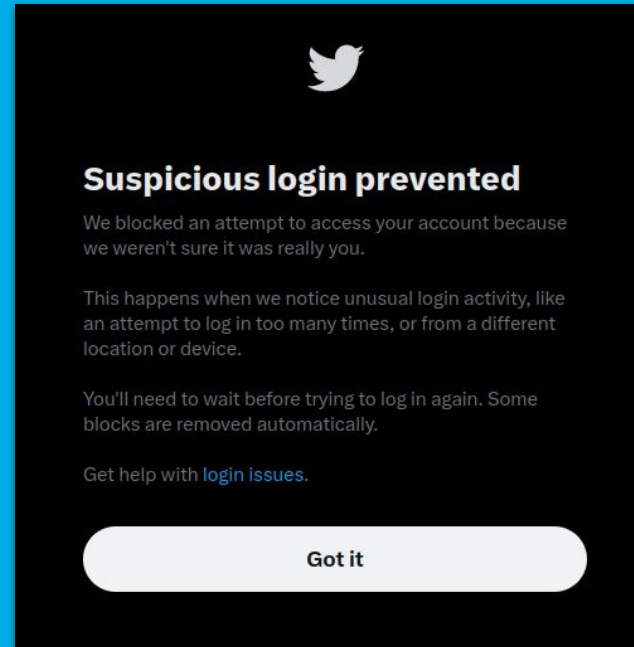
# What is Twitter?

- 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



**Create your account**

Name  
Tadeas

Email  
koubatad@cvut.cz

Email has already been taken.

**Find your Twitter account**

Enter the email, phone number, or username associated with your account to change your password.

Email, phone number, or username  
nonexistentemail@email.com

Next

Sorry, we could not find your account.

# Password Check Inconsistent



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

Current password

.....

[Forgot password?](#)

New password

.....

That password is too easy to guess. Please choose a stronger password.

Confirm password

.....



# 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

```
{  
  "email": "ehapentesttwitter3@proton.me",  
  "email": "Mr. Pentester",  
  "flow_token": "g;168708217759848894:-168719172166.  
}
```

## Response

	Pretty	Raw	Hex	Render
1	HTTP/2 500 Internal Server Error			
2	Date: Mon, 19 Jun 2023 16:53:47 GMT			
3	Perf: 7626143928			
4	Pragma: no-cache			
5	Server: tsa_o			
6	Expires: Tue, 31 Mar 1981 05:00:00 GMT			
7	Content-Type: application/json; charset=utf-8			



Thank you for your attention

Any questions?