COMP64 [illegible] eek 2)

Use [illegible] tion

sec edu

A NOTE ON ETHICS / LEGALITY

- UNSW hosting this course is an extremely important step forward.
- We expect a high standard of professionalism from you, meaning:
  - Respect th he university
  - Always abide by the law an regulations
  - Be considerate of others t yone has an equal learning experience
- Always check that you have written permission before performing a security test on a system

PLEASE BE SUPER CAREFUL WHENEVER YOU’RE GENERATING NETWORK TRAFFIC

“NOT-A-HOMEWORK”

What tools have you tried?

“NOT-A-HOMEWORK”

What tools have you tried?

- Burp
- Fiddler
- Wireshark
- nMap
- Nikto
- ZAP

“NOT-A-HOMEWORK”

What have you seen?

- Requests
- Messages head
- Files
- Page layouts

IDENTITY

What is IDENTITY?

IDENTITY

What is DIGITAL identity?

- A digital ide n entity used by computer syst nal agent
- ISO/IEC 24760 ated to an entity"
- Various National digital ide s

IDENTITY ATTACKS

- Social
- Credential stealing
- Compromised/weak password
- MitM

OWASP TOP TEN

https://owasp.org/www-project-top-ten/

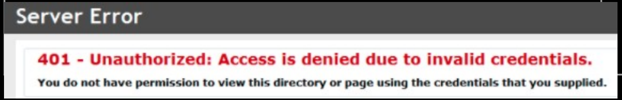
OVERVIEW

Authentication → Session Management → Access Control(Authorization)

Is the user who they claim to be? If not

that us

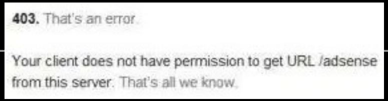
Is the user llowed to access this thing?



Server Error

401 - Unauthorized: Access is denied due to invalid credentials.

You do not have permission to view this directory or page using the credentials that you supplied.



403. That's an error.

Your client does not have permission to get URL /adsense from this server. That's all we know.

WEB AUTHENTICATION 2021

- Username / Pas
  - Password reset via email
  - 2FA: SMS, Token, Apps (incl TOTP)
  - Active vs Passive 2FA
- Authentication can be delegated (e.g. SSO, Oauth, JWT)
- CAPTCHAs

BAD AUTHENTICATION 101

BAD AUTHENTICATION 101+1

BAD AUTHENTICATION 101

DEFAULT CREDENTIALS

> “The ASD's investigation found that internet-facing services still had their default passwords, admin:admin and guest:guest.”

http://www.zdnet.com [illegible]-data-stolen-in-australian-defence-contrac [illegible]

BRUTE FORCE (BEST FORCE)

- Attempt logins with common passwords
- Try known email + password combinations from previous breaches
  - 1 User, Man
  - Many Users, tial Stuffing”
- Login rate-limiting and locko
  - CAPTCHA
  - Lockouts (iPhone)
- Proactive Monitoring
- User Communication

INFORMATION DISCLOSURE

“Logi name.”

“Login failed: invalid u password.”

ERRORS HANDLING

ERRORS HANDLING

asp.ne ion-timeout

TRANSPORT LAYER SECURITY (WHY?)

MitM attack: forces a victim's browser into communicating with an adversary in plain-text over HTTP, and the adversary proxies the modified content from an HTTPS server

WIFI PINEAPPLE

Pen testing device for man-in-the-middle attacks

WIFI PINEAPPLE

Pen testing device for man-in-the-middle attacks

https://www.youtube.com/watch?v=fm-J_ITox5w

PASSWORDS

WHAT IS ~~LOVE~~ HASH?

One way function

HASHING vs ENCRYPTION

HASHING vs ENCRYPTION

Hash algorithm is based on one-way function. It is practically impossible to revert the result back

Encryption is based on plain text and a key and suppose to have a decryption algorithm.

PASSWORD HASHES

RAINBOW TABLE AND PASSWORDS DBS

https://haveibeenpwned.com/Passwords

passwords ob data breaches

DEMO

https://youtu.be/IchpQBbGbrE

PASSWORD RESETS

- E-Mail
  - Doesn’t matter if I’ve got the user’s inbox
  - Is the reset link generated securely?
  - Can I gene
- “Security” Questions
  - Can I get them off a user
  - Can I google the answer?
  - How many attempts do I get to answer these questions?

Password Security is
People Problem

2019 NIST PASSWORD GUIDELINES

8 character min (human) overwise 6 character min

* Support at least 64 characters max length

* support All ASCII characters (incl 0x20)

* NO truncation o d

* Allow at least ore lockout

* No SMS for 2FA (one-time passw app)

- Check password with known dictionaries
- No complexity requirements
- No password expiration period
- No password hints
- No knowledge-based authentication (no questions)

Few more examples

Shout out: 0xed1337

Few more examples

Shoutout: T-GOX Channel

How to do Good authentication?

- Good password policy
- Rate limiting
- Not allowing default usernames/passwords
- Not using we
- Multi Factor
- Application registration/fo ord logic

READING MATERIAL (REFERENCE)

- Authentication what why and how!!
  https://github.com/alex996/presentations/blob/master/auth.md

- Shopify Authe
  https://www.youtube.com/wat -r-9Lg

- Google CTF
  https://www.youtube.com/watch?v=HOQzu0SQFWA

WEEK 2-3 ASSESSMENT

- If you’re unsure, ask.

Please call out if you get stuck.
Support one another, your tutors are here to help!

THAN TO US

questions? email ing