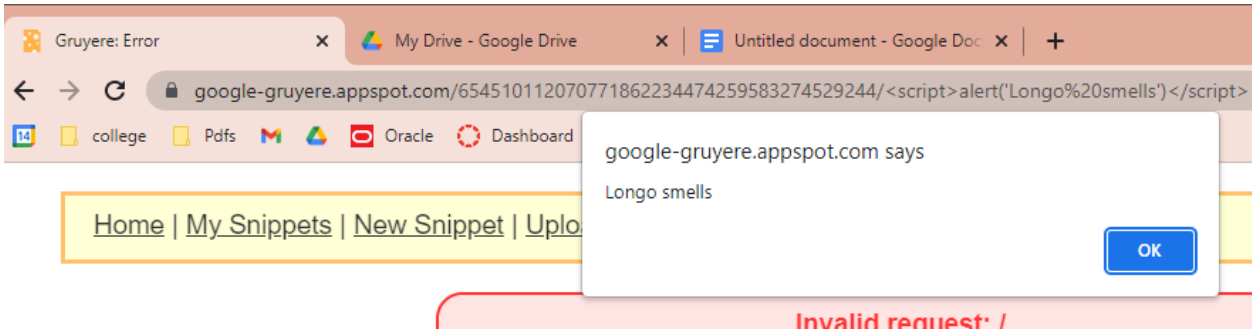
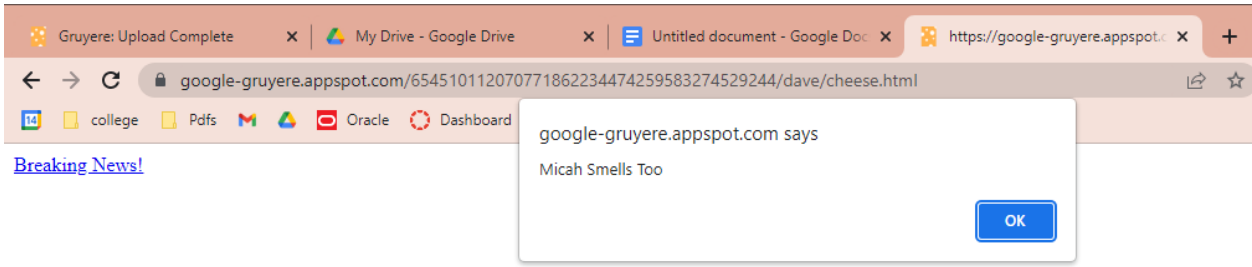
David Thomsen

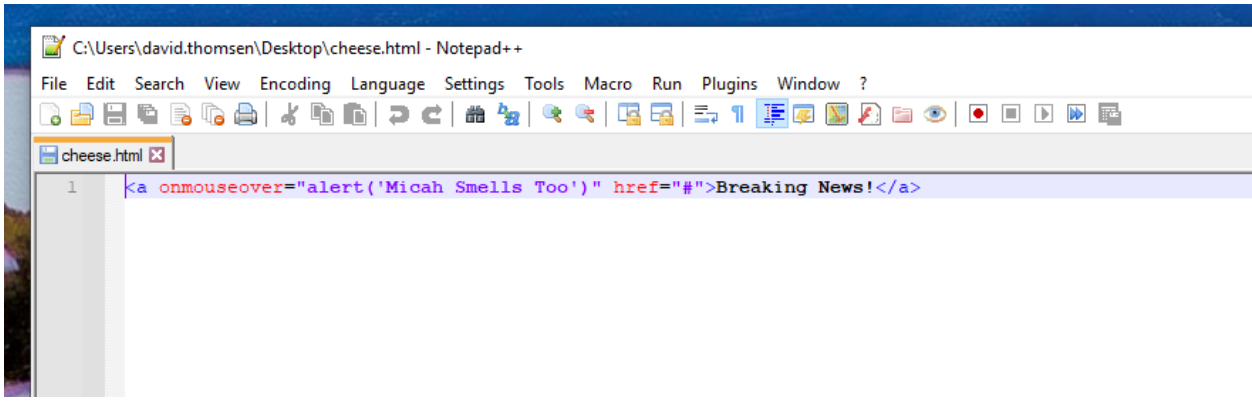
SEC-260

Challenge 1 - XSS

On the right side of the Codelab page, you will find links to challenges. To further understand XSS techniques, complete the following 3 challenges:

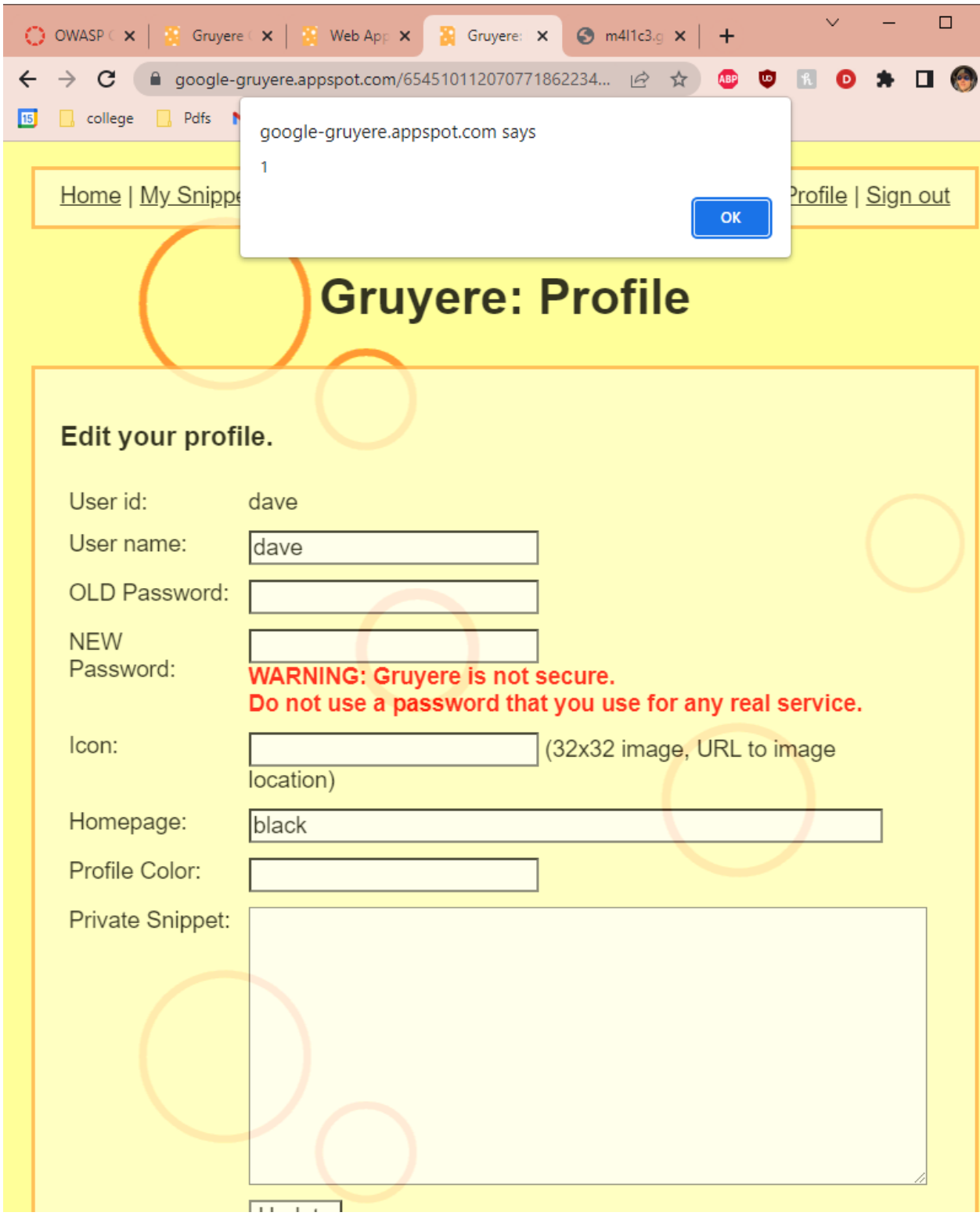
1. Reflected XSS
    a. 

2. Stored XSS
    a. 

    b. 

3. Stored XSS via HTML Attribute

a.

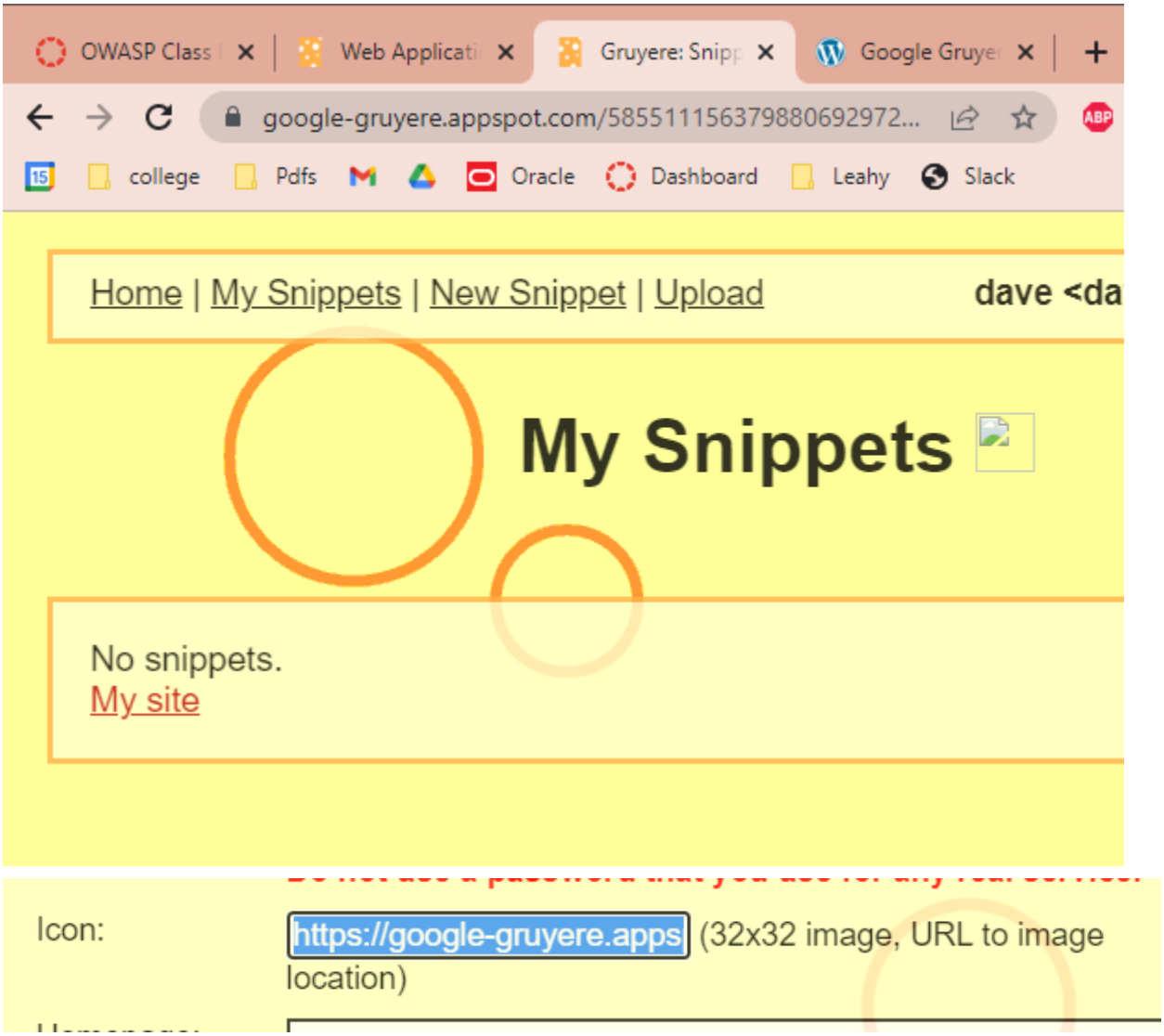

google-gruyere.appspot.com/654510112070771862234...
college
Pdfs
google-gruyere.appspot.com says
1
OK
Home | My Snippe
Profile | Sign out
Gruyere: Profile
Edit your profile.
User id:
dave
User name:
dave
OLD Password:
NEW Password:
WARNING: Gruyere is not secure.
Do not use a password that you use for any real service.
Icon:
(32x32 image, URL to image location)
Homepage:
black
Profile Color:
Private Snippet:

b.

Challenge 2 - XSRF

Find a way to trick someone into deleting one of their Snippets

Submit:



1. https://google-gruyere.appspot.com/5855111563798806929723389572157802763 85/deletesnippet?index=0
    a. **(could disguise this with a bit.ly, didn't so you can see the syntax.)**

Screenshot demonstrating the CSRF exploit

Brief description of how CSRF and XSS can be used together

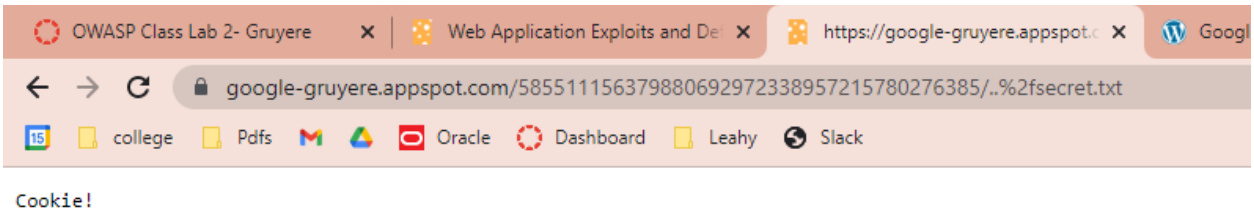
By using XSS to create a link that may end up causing harm to a user's account or data, you can use CSRF to disguise it as another link or make it less obvious that it is malicious.

Challenge 3 - Information Disclosure by Path Traversal

See if you can read the contents of the "secret.txt" file on the Gruyere server using a path traversal attack. Hint: you will likely need to use percent encoding to specify the path in the browser

Submit:

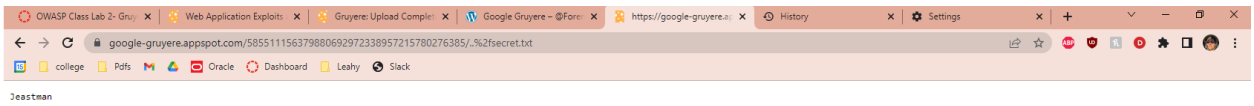
Screenshot of the secret.txt file contents



What was the URL you used to access the file?

google-gruyere.appspot.com/984698340982348957230984 98/..%2fsecret.txt

Challenge 4 - Data Tampering by Path Traversal



Follow the challenge hints and see if you are able to overwrite the existing secret.txt file with a new one that you created.

Hint: After you replace the secret.txt file - try and load it from a different browser session as there seems to be some session issues that will keep the old file loading even if you clear the cache.

Submit:

Screenshot of the new secret.txt file contents being served by the Gruyere app

Briefly describe how an attacker could use this file replacement vulnerability to compromise a web server

An attacker could use this vulnerability to replace key files that make the web server operate, or they can use it to keep a back door open if they want to get back into the server at some point.