Web Service Attacks

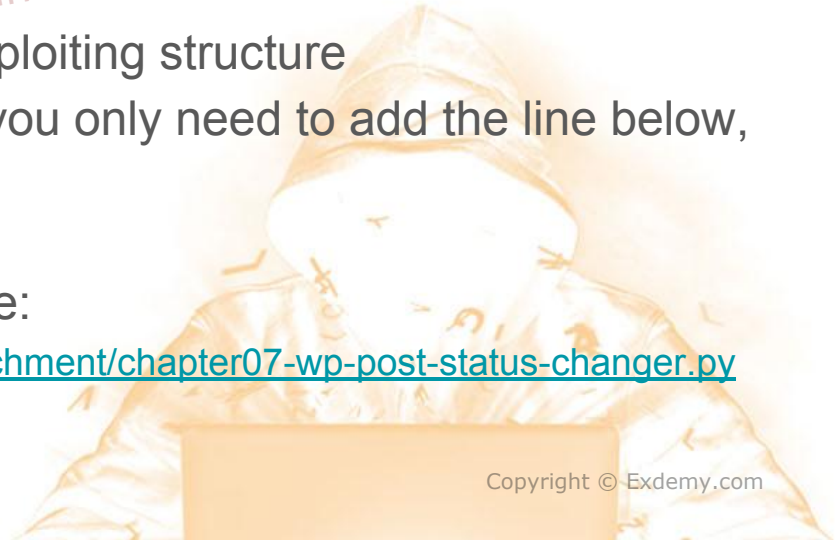
WordPress Content Injection

Wordpress Content Injection

- Create an exploit to change the post status to **drafted** using the Wordpress Content Injection base exploit
- If you didn't set up the vulnerable Wordpress locally, use the online lab

Wordpress Content Injection - Solution

- First of all you need to look at the REST API documentation to figure out what parameters you can use
  - https://developer.wordpress.org/rest-api/reference/posts/#update-a-post
- The status parameter can have 4 different value:
  - publish, future, draft, pending, private
- Also the base exploit helps you use the exploiting structure
- To add status change to the basic exploit you only need to add the line below, i.e. replace line 61 with:
  - 'status': 'draft'
- You can download the full exploit from here:
  - https://exdemy.com/advanced-web-hacking/attachment/chapter07-wp-post-status-changer.py



ZDResearch Advanced Web Hacking

ZDResearch

www.zdresearch.com