NC STATE UNIVERSITY

CSC-295
HackPack

Alexandros Kapravelos

akaprav@ncsu.edu

Administration

- Class website
  - https://kapravelos.com/teaching/csc295-f20/schedule/
- Slack channel
  - https://ncsu-hackpack.slack.com/
- Mail to instructor
  - Subject: [CSC-295]
  - akaprav@ncsu.edu
- Recorded classes
  - https://mediasite.wolfware.ncsu.edu/online/Catalog/Full/1ed72d833c494613aba1feefb0abcde72120

Material

- What material will we be using?
  - Unfortunately, there is no good book to follow on hacking
    - (optional) **The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws**
    - (optional) **The Tangled Web: A Guide to Securing Modern Web Applications**
  - Use the slides that I will post on the web site
  - Related papers/readings and online material (from the syllabus)

Grading

- No exams
- Six weekly writeups -> 100% of your grade
- No participation grade (due to COVID)

Topics

- Practical hacking
- Focus on web security specifically
- **How to identify and exploit web vulnerabilities**
- Solve CTF challenges

You need to understand

- 90% of hacking is **exploring**
- You will need to build attacks. I expect you to:
  - know how to code (in language of your choice*)
  - I will use mix of pseudocode, Python, JavaScript, PHP
  - be(come) comfortable with Linux/UNIX

Goals

- **Teach adversarial mindset**
- Discover security vulnerabilities in web applications
- Exploit web vulnerabilities
- Work with specific tools and methods, but understand the mechanics underneath

Assignments

- Individual weekly assignments
- Read a CTF writeup and suggest improvements
- Work on the weekly challenge and exploit it
- Write your own writeup
- Discovering a vulnerability is a frustrating, but very rewarding in the end!
- The best writeups will be published on https://hackpack.club/writeups

CTF participation

We are going to participate in three live CTFs!

1. Google Capture The Flag 2020
   22 Aug., 00:00 UTC — 23 Aug. 2020, 23:59 UTC
2. CSAW CTF Qualification Round 2020
   11 Sept., 20:00 UTC — 13 Sept. 2020, 20:00 UTC
3. TokyoWesterns CTF 6th 2020
   19 Sept., 00:00 UTC — 21 Sept. 2020, 00:00 UTC

CTF participation

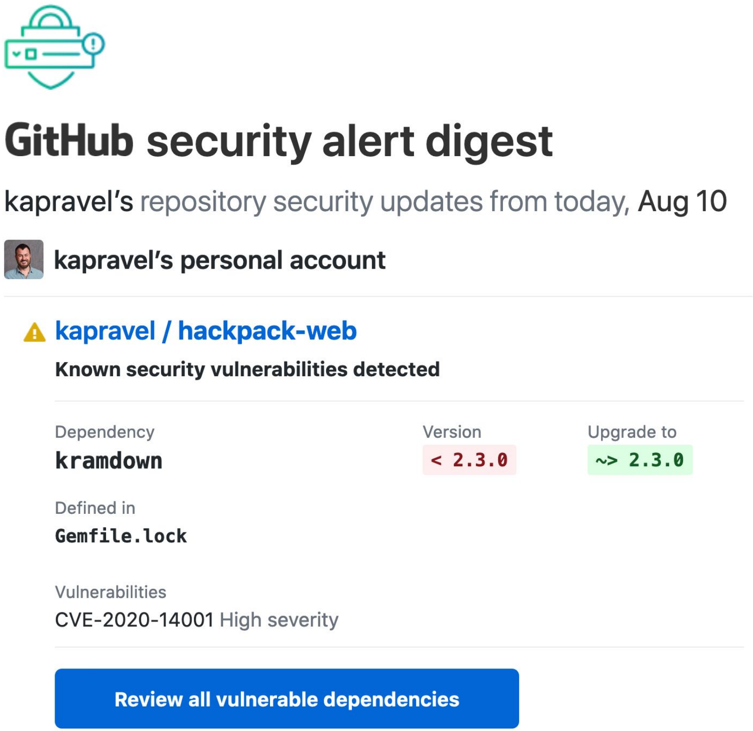
- Pair hacking
  - Everyone needs to pair with someone else when playing CTFs
- Coordination will happen over slack

Preparation for next week

- Chrome Dev Tools
  - Overview
  - Debugging JavaScript - Chrome DevTools 101
- Burp Suite Training
- Set up an environment were you can debug web applications easily
  - Inspect & modify cookies/headers/requests/code
  - Debug JavaScript
- Spawning this environment should be **scripted**
  - bash/docker/ansible/vagrant

Your Security Zen

Vulnerabilities are everywhere



GitHub security alert digest

kapravel's repository security updates from today, Aug 10

kapravel's personal account

⚠ kapravel / hackpack-web

Known security vulnerabilities detected

Dependency	Version	Upgrade to
`kramdown`	`< 2.3.0`	`~> 2.3.0`

Defined in
`Gemfile.lock`

Vulnerabilities
CVE-2020-14001 High severity