Ethical Hacking 200

Assignment 7-2: Using fundamental understanding to find Web Vulnerabilities

Contents

Recap

In class we covered various vulnerabilities in depth. We also revisited the HTTP protocol as we analyzed from end to end what an attacker considers attacking when trying to achieve a goal (e.g.: everything that happens when a "webpage is given to a user"). We also went into depth on what HTTP headers are. As always you should take these fundamental concepts to then apply them in further scenarios. In this case finding a vulnerability in a new situation.

Your Assignment:

- **Learn to Edit and Run Python Scripts –** if you have not already. The scripts were written in python version 3.7.9, as such run it using at least python3. https://www.python.org/downloads/
- **Find the vulnerability –** This time we are not telling you what you are looking for. In a real setting a client never tells you want issues to find in their products. You should:
  - Run "run_hidden.py" and then visit http://localhost:8000 in your web browser
    - A proxy tool such as owasp zap, fiddler, burp, etc can help here but is completely not needed. Keep in mind tools are for efficiency and should never be a replacement for your skill and understanding.
    - To view the requests being sent you can use the "developer tools" in your web browser. Safari Chrome Firefox etc
      In short, right click and inspect/developer tools. Go to the network tab, make sure to check "preserve log" so you don't lose the history of what request have been observed. Then start playing with the webpage and see what traffic goes out.
      or
      https://www.google.com/search?q=youtube+network+tab+in+developer+tools

        - Play with the application normally first and try to make educational guesses in your mind as to how it is working
        - As you start to experiment, *pay very close attention to differences in behavior*.
            - It might even help to write down things you notice, to then take a step back and see if you can see something larger going on. Putting a list of your observations next to what you think the application is doing and how you think it might be working might give you a larger picture.
        - Combine anything you observe with your fundamental understanding you have built up till now. What could those behavioral differences mean, in what way might you use it to your advantage as an attacker?
        - Keep in mind you are looking for realistic issues. For example “I as an attack can modify a file and email it to a victim” is not realistic *in this scenario*. You want to be able to have the user visit the application themselves, such as giving them a link to visit, and that attacks the user/application.

What to turn in:

- What vulnerabilities/Issues did you find?
    - A short description, a sentence or two for each
      (there will be at least 2 core vulnerabilities)
        - what is the vulnerability/problem (1 pts x 2 vulns)
        - what is the payload/attack (1 pts x 2 vulns)
        - what observation you made which lead to you finding the issue (1 pts x 2 vulns)
        - the impact of the issue for a victim/user (1 pts x 2 vulns)
        - how you would fix the problem (1 pts x 2 vulns)
- Technically there is more than one vulnerability, but you will end up using them together for a larger attack/impact.
    - Technically there is more than one way to attack this. This next statement will make more sense as you dig into the application:
      You can use the “comment” to get to a next step, however this is slightly unrealistic and a bit gamified, though still educational. For a more realistic experience try to find an attack other than the one using the “comment”. If you do end up using the “comment” it is not a reduction in points, not using it is simply challenging yourself.
- Any reasonable text format is acceptable

Im having a really hard time!

As always, the best thing you can do is reach out as early as possible to the instructor.

Feel free to discuss in group chat, but please do not give out examples or answers. An appropriate level of information in group chat would be sharing information sources discovered (e.g: hey I found this nice explanation on what “bits” vs “bytes” are). However, you should NOT directly address answer in group chat (e.g: hey did you know “x0b” on line 37 means…). It should be up to each student to read, absorb information, and build up and then apply their own practical skills to be able to do this on their own.

Hints

Using hints will make finding the vulnerability less realistic but using them will not reduce the points you can earn on the assignment. If possible, try not to use the hints to challenge yourself and gain the most value out of this exercise. While it isn’t a fun lesson, wracking your brain and exhaustively thinking through a problem, burning large amount of time, is a very valuable lesson. Cumulatively overtime this becomes experience and eventually intuition, efficiency, and a steppingstone to tackling finding really deep-rooted vulnerabilities. You get good at solving puzzles, by solving puzzles.

The hints are in levels 1-4, 1 being the least amount of help and 4 the most. None of them will completely give you the answer, but the higher the level the more it will tell you what to do, and the less realistic solving the puzzle becomes. “**<u>Base64 decode” the hint text to see the hints.</u>**

Hint – Level 1: Using this hint will let you know what vulnerability you are looking for.

WW91IGFyZSBsb29raW5nIGZvciBhIFhTUywgeW91ciBnb2FsIGlzIHRvIHBvcCB1cCBhIGFsZXJ0KCkgYm94IH
dpdGhvdXQgdGhlIHZpY3RpbSBtYW51YWxseSBkb3dubG9hZGluZyBhbmQgb3BlbmluZyBhIGZpbGUuCkFzI
GFuIGF0dGFja2VyIHlvdSB3YW50IHRvIGJlIGFibGUgdG8gZ2l2ZSB0aGUgdmljdGltIGEgbGluayB0byB2aXNpd
CB0byB0aGVuIGludGVyYWN0IHdpdGggdGhlIGFwcCwgYW5kIHRoZSB4c3MgYXR0YWNrcyB0aGVtLiBUaGl
zIHdheSB0aGUgeHNzIGV4ZWN1dGVzIG9uIHRoZSAiZG9tYWluIiBvZiB0aGUgYXBwbGljYXRpb24uIA==

Hint – Level 2: Using this hint will make it even less realistic. You will still have to figure out what to do, but it tells you where to look.

SWYgeW91IGRvbnQga25vdyB3aGF0IGEgaHR0cCBoZWFkZXIgZG9lcywgbG9vayBpdCB1cC4KYnJpbmdpbm
cgYXR0ZW50aW9uIHRvIGh0dHAgaGVhZGVycyBpcyBhIGhpbnQgaW4gaXRzZWxmLiA=

Hint – Level 3: Using this hint will make it even further unrealistic. This will tell you where to look and what to do without completely giving you the answer.

QXMgeW91IHBsYXkgd2l0aCB0aGUgYXBwbGljYXRpb24sIHBheSBhdHRlbnRpb24gdG8gdGhlIEhUVFAgaGV
hZGVycyBvZiByZXF1ZXN0cyBnb2luZyBvdXQgYW5kIGlmIHRoZXJlIGFyZSBhbnkgc3BlY2lmaWMgYmVoYXZp
b3JzIHlvdSBvYnNlcnZlLgppcyB0aGVyZSBhbnl0aGluZyB5b3UgY2FuIGNvbnRyb2w/

Hint – Level 4: Using this hint basically will tell you what the first vulnerability is, but at the least will not tell you what to type. You still have to figure some things out.

TG9vayBmb3IgdGhlIEhUTUwgY29tbWVudCBpbiB0aGUgZmlsZSB5b3UgZG93bmxvYWQuCkl0IHdpbGwgY
mUgYSA8IS0tIHNvbWV0aGluZyAtLT4KVGhpcyBpcyBhIGtleSBwYXJ0IG9mIHRoZSBhcHBsaWNhdGlvbiBsb2
dpYywgb2YgdGhpbmdzIGl0IGlzIGRvaW5nIGJlaGluZCB0aGUgc2NlbmVzLiAKRmlndXJpbmcgdGhpcyBvdXQ
gd2lsbCBsZXQgeW91IGdldCB0byB0aGUgbmV4dCBzdGVwIHRvIGFjdHVhbGx5IHN0YXJ0ICJleGVjdXRpbmci
IHNvbWUgamF2YXNjcmlwdCBmb3IgeW91ciBYU1Mu