14-741/18-631: Homework 5

All sections Due: Thursday November 4, 2021 by 10:00am EST

Name:

Andrew ID:

Total (100 pts max):

Guidelines (Please read before starting!)

- Be neat and concise in your explanations.
- You must use at most one page for your explanation for each Problem (code you wrote may be on additional pages). Start each problem on a new page. You will need to map the sections of your PDF to problems in Gradescope.
- To access the CTF problems, create the SSH proxy as per the guide on Canvas.
- For CTF problems, **you must use the following format in your explanation**:
  - CTF Username
  - Flag
  - Explain the vulnerability in the program, and explain conceptually how that vulnerability can be exploited to get the flag.
  - How did you exploit the vulnerability? List the steps taken and the reasoning behind each step. The TA grading should be able to replicate the exploit following the steps. Feel free to make references to your code! **Note that *"use XYZ online solver"* is not sufficient - you must explain how the online solver derived the answer for full credit.**
  - Append your source code in the same writeup. Your source code should be readable from the writeup PDF itself. Note that this does not count towards the page count above.

  Omitting any of the above sections would result in points being deducted.
- Some questions are marked as **Optional Team Work**. For those, you can work with another student. The maximum team size is 2. In your write up, please write "completed as a team" for the designated team work problem, followed by the andrew ids of you and your teammate. **Individual CTF username and flag need to be put in the write up for CTF questions.** Please refer to the problem write up for requirements of whether to submit individual or one joint write up (this may defer from problem to problem).
- **References:** List resources outside of class material that helped you solve a problem. This includes online video tutorials, other CTF problems on other platforms, etc. Remember that source code available online (e.g. stackoverflow) also needs to be cited. A quick guide on citing source code can be found here: `https://integrity.mit.edu/handbook/writing-code`. **Omitting the references section may result in an Academic Integrity Violation(s).**
- It is highly recommended that you use Python for your assignment. You may use other languages that you are familiar with, but the teaching team will not be able to support or debug language specific errors.
- Please check your English. You won't be penalized for using incorrect grammar, but you will get penalized if we can't understand what you are writing.

- Proofs (including mathematical proofs) get full credit. Statements without proof or argumentation get no credit.
- There is an old saying from one of my math teachers in college: "In math, anything partially right is totally wrong." While we are not as loathe to give partial credit, please check your derivations.
- Write a report using your favorite editor. Note that **only PDF submissions will be graded.**
- Submit to Gradescope a PDF file containing your explanations and your code files before 10:00am Eastern Standard Time on the due date. You can find the timing for EST here: `https://time.is/EST`. Late submissions incur penalties as described on the syllabus (first you use up grace credits, then you lose points).
- If you choose to use any late days, you do not have to inform the instructors. We will calculate the number of late days used at the end of the semester based on the time of submission on Gradescope.
- Post any clarifications or questions regarding this homework to Piazza.
- **General allowed team work** Beyond designated team questions, you are encouraged to shared resources (e.g., TA's help, online resources you found helpful); you are encouraged to set up virtual study sessions with your teammate(s) to check each other's progress and discuss homework assignment solutions.
- **This is not a group assignment. Beyond your teammate, feel free to discuss the assignment in general terms with other people, but the answers must be your own.** Our academic integrity policy strictly follows the current INI Student Handbook `http://www.ini.cmu.edu/current_students/handbook/`, section IV-C.
- Good luck!

1 XSS (25 points)

To solve this problem and extract the flag, you need to execute Javascript in the context of "overlords" on a website vulnerable to XSS. You are expected to use Cross Site Scripting to get the flag for full points. Other types of exploits such as HTML Injection while possible would result in only partial credit. Submit a writeup containing:

1. CTF username
2. the type of XSS
3. explanation of how your XSS exploit works
4. the payload
5. the flag

2 SQL Injection (20 points)

Solve the SQL Injection problem on the 14741 CTF Server. Submit a writeup containing:

1. CTF username
2. which fields are injectable? which not? (prove from challenge source code)
3. explanation of vulnerability
4. steps taken
5. flag
6. code (with comments!) you used, if any

3 Blind SQL Injection (30 points) (Optional Team Work)

You can choose to form a team of 2 students or work individually. If you are working in a team, only one needs to author the write up, and the other simply writes "*see [teammate's andrewid]*". Note that for all other questions in this homework assignment, you have to write your own answers.

Solve the SQL Injection 2 problem on the 14741 CTF Server. Submit a writeup containing:

1. CTF username
2. which fields are injectable? which not? (prove from challenge source code)
3. explanation of vulnerability. How is this different from the previous SQL Injection?
4. steps taken
5. flag
6. code (with comments!) you used, if any

4 SQL Injection (Android) (25 points)

We have an android app using SQL database. We don't need to worry about SQL injections, right? Note that you need to hide the keyboard before you press the login button for the application to work properly. Solve the SQL Injection problem. Submit a write up containing:

1. CTF username
2. which field(s) did you use to exploit the vulnerability?
3. explanation of vulnerability.
4. steps taken
5. flag
6. code (with comments!) you used, if any