ID 2018963

Exam for 06-30195 Security and Networks

After inserting your student ID and the module name in the title, header and footer, write your answers between here and the statement of good academic conduct. Your ID and the module name will automatically appear on any subsequent pages.

Question1

(a) SQL injection, Broken Authentication and Arbitrary Command Execution.

SQL injection: The attacker successfully submitted the malicious SQL query code to the server. After receiving the program, the program mistakenly executed the attacker's input as part of the query statement, causing the original query logic to be changed, and the malicious code constructed by the attacker was additionally executed.

Broken Authentication: The website does not use SSL/TLS encryption, and when the user is using general network, the attacker uses the sniffer to eavesdrop to obtain the user ID, session ID, etc., and further log into the account.

Arbitrary Command Execution: the parameter of password(pw) can be controlled, and will be executed as a command. And then arbitrary commands will be executed after the attacker constructs the system.

(b) The password has to encrypt before stored. And the password is in plain text, may lead to account leakage(especially when database is leaked)

Solution: use bcrypt or PBKDF2 algorithm which are specially designed for encrypting passwords.

(c) The attacker will insert some malicious script code into the web page. When the user browses the page, the script code embedded in the web page will be executed which can achieve the purpose of attacking the user. Then even if the user doesn't download any malware, they will be attacked.

Question2

(a) ALSR(Address space layout randomization) and NX

ALSR will change the binary's base address every time the binary starts which is hard for attackers to get correct address.

NX-bit

It is used to divide the memory area into only for storing the processor instruction set, or only for data use. So it can prevent most buffer overflow attacks, some malicious programs

put their own malicious instruction sets in data storage area of other programs and execute them, thereby controlling the entire computer.
Normally, the 2 mechanisms will be activated together and will work together. It's impossible for an attacker to locate their shellcode location correctly. Even the attacker has the shellcode location, it's impossible to execute it as well.

(b)It compares the first six bytes of string command with the string "reboot", and they are totally the same(return), then reboot.
SQL injection, since the user doesn't know the password, so just enter 'OR'1'=1='1 for password, and when querying whether the username and password are correct, SELECT * FROM user WHERE username='' and password='' was originally executed. After the parameters are spliced, the SQL statement SELECT * FROM user WHERE username='' and password= will be executed. '' OR '1'='1', at this time 1=1 is true, so the verification will be skipped naturally.
Repair code:
Line8 from gets() to fget()

(c)Yes. The attacker still cannot get the location of the shellcode.

Do not write below this line

Statement of good academic conduct

By submitting this assignment, I understand that I am agreeing to the following statement of good academic conduct:

- I confirm that this assignment is **my own work** and I have not worked with others in preparing this assignment.
- I confirm this assignment was written by me and is in my own words, except for any materials from published or other sources which are clearly indicated and acknowledged as such by appropriate referencing.
- I confirm that this work is not copied from any other person's work (published or unpublished), web site, book or other source, and has not previously been submitted for assessment either at the University of Birmingham or elsewhere.
- I confirm that I have not asked, or paid, others to prepare any part of this work for me.
- I confirm that I have read and understood the University regulations on plagiarism (https://intranet.birmingham.ac.uk/as/registry/policy/conduct/plagiarism/index.aspx).