Computer Security Fundamentals – Spring 2023

System and Networks Security **Total: 15 points**

Q1. XSS attack (2 pts)
For XSS attack, there is a common approach to look for injectable fields.
In my slides, there is a way to identify injectable fields, can you briefly talk about that? (1 pt)
[Hint]: We can identify if this website can support the execution from user's input of some language as well as seeing if this field can be stored or saved? **(2 criteria need to be satisfied at the same time!)**

In our Truman's website, https://www.truman.edu/
, there is a search field.

Is this an injectable filed? (1 pt)

Q2. XSS attack (1 pt)
In my slides, there are 2 types of XSS attack, what are they? (0.5 pt per each)

Q3. Beef Framework and XSS (1 pt)
In the XSS attack we introduced in the class, there is a very evil file inside of the Beef browser exploitation framework, what is it? (1 pt)

Q4. XSS process (1 pt)
What is the process of the XSS attacking example we introduced in the classroom?
Can you briefly talk about that?
[Hint]: Please refer to a flow of attacks in my slide

Q5. Google Phishing and Pretty Theft (1 pt)
Can you briefly describe how these 2 modules in the Beef framework, if they get launched in end user's browser, how does it look?

Q6. NoSQL Injection (2 pts)
What is payload? (1 pt)

Why hackers like to modify the payload and send it to the server?
Can you briefly tell me the purpose or anything knowledge behind? (1 pt)

Q7. NoSQL Injection (1 pt)
It is not likely that we can interact with the NoSQL directly. Isn't it?
The only one thing we can do is to exploit the vulnerability of WebAPI. (WebAPI can interact with NoSQL)
In my slides, I demonstrated an example by setting "$ne": -1 and apply this on "id"
Obviously, "$ne" is from something in the MongoDB (if you took my Database course in Fall 2022)

Here is the quote in MongoDB references.
"$ne selects the documents where the value of the field is not equal to the specified value"
https://www.mongodb.com/docs/manual/reference/operator/query/ne/

Now you need to tell me, if we applied "$ne": -1 on the "id" field.
What is going to happen? If there is anything knowledge behind?

Q8. sqlmap (1 pt)

In the class we talk about the command of “sqlmap”. It is about the SQL injection.
Briefly tell me how it works? Or? What are the functions it has?

Q9. HTTP response code (1 pt)

When we are performing reconnaissance or attacks, observing the http response code from the server is important. We need to know what are activities counted as “**legitimate**”?
There are **5 categories** of http response code.
Can you briefly talk about all of them by using your own words? (I only like to know the 5 categories, not the details on all of them)
You know, this is very important in the process of hacking but is also crucial in the development of client-server, distributed systems.
Hint: Here is an example website talking about the response code
https://developer.mozilla.org/en-US/docs/Web/HTTP/Status#successful_responses

Q10. SSH attacks (2 pts)

nmap is a command we had learned earlier, it is not just a tool to scan someone’s device but also an attacking tool. In the class, we introduced the way to use nmap to perform port 22 (SSH) attack by using dictionary files (user name and password). Can you briefly talk about how to do this? (1 pt)

In the SSH attacks, we introduced “hydra” and “hydra-wizard”. What is the benefit to use the “hydra family” compared the uses with nmap brute-force attacks? (1 pt)

Q11. Burp Suite (1 pts)
In the Burp Suite, there is a very "**evil**" tab with some functions called "**Intruder**".
So the hackers can easily change the payloads here and sent it to the attacking target by using a right click on the request → [Send to Intruder]

Under the "Intruder tab", as our demonstration in the classroom, we switched from the "Positions" tab to "Payloads" tab. We use "root" account as our #1 payload field and **we set the type** as "**Simple List**"

Now, in order to process the #2 payload field, the password field, we choose a file from our "metasploit" installed in our Kali Linux machine. Then, what is the "**payload type**" we just set for this 2nd field of payload?

Q12. Metaspolit (1 pt)
In our demo, we use metasploit as a tool to conduct our SSH attacks.
So tell me, **in your own words, not just 1 or 2 sentences.**
Briefly describe what are the things the metasploit can do in helping us in the SSH attacks?