Name: SUMIT PANDA

Reg : 11718492

Question 1: Using an appropriate tool, evaluate whether your organization is vulnerable to SQL injection attack or not? Explain the process required?

Step1: We need a Linux based system

Step2: We can sql map via two ways i. We can use the python file ii. We can install sqlmap directly into the system.

Step3: To install the in the system we have to run a command like

→sudo apt-get install sqlmap

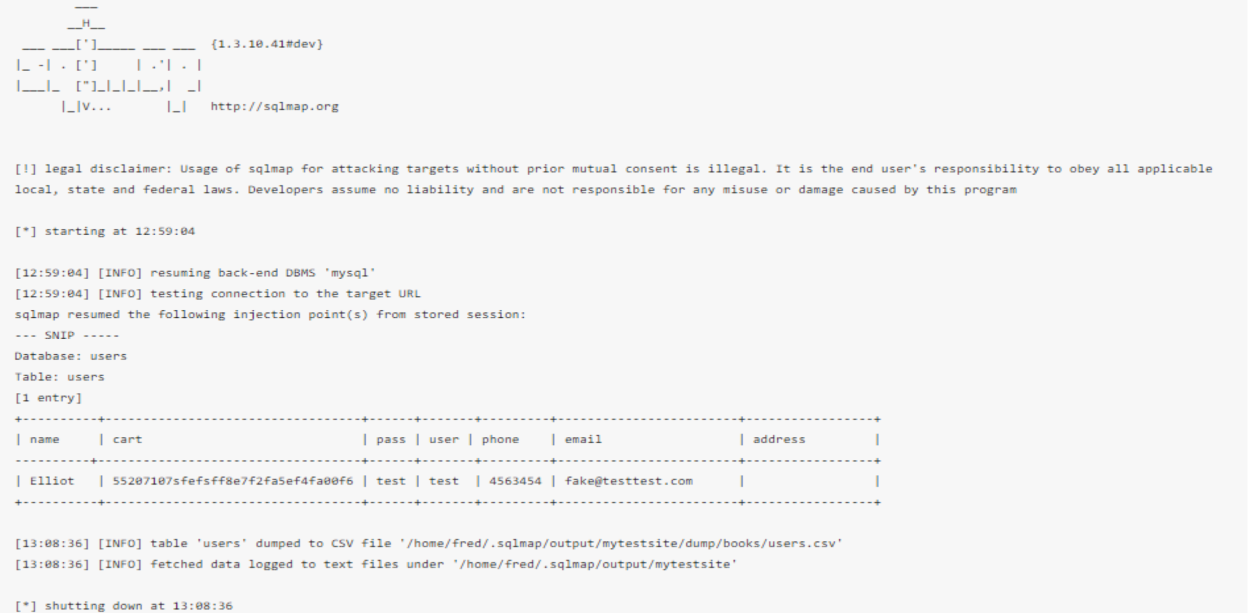
Step4: Now we need a testing subject, it can be the website of the organization.

Step 5: Now we have to run the tool over the site like

→sqlmap -u 'www.mytestsite.com/page.php?id=5' --tables

// this command will scan the site and will look for the data tables.

** here I am taking an example and attaching with the sample output with it.



```
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.3.10.41#dev}
|_ -| . [']     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org


[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 12:59:04

[12:59:04] [INFO] resuming back-end DBMS 'mysql'
[12:59:04] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
--- SNIP -----
Database: users
Table: users
[1 entry]
+----------+----------------------------------+------+-------+---------+-----------------------+----------------+
| name     | cart                             | pass | user  | phone   | email                 | address        |
----------+----------------------------------+------+-------+---------+-----------------------+----------------+
| Elliot   | 55207107sfefsff8e7f2fa5ef4fa00f6 | test | test  | 4563454 | fake@testtest.com     |                |
+----------+----------------------------------+------+-------+---------+-----------------------+----------------+

[13:08:36] [INFO] table 'users' dumped to CSV file '/home/fred/.sqlmap/output/mytestsite/dump/books/users.csv'
[13:08:36] [INFO] fetched data logged to text files under '/home/fred/.sqlmap/output/mytestsite'

[*] shutting down at 13:08:36
```

Step 6: Now I have the result, and based upon the output/result I have to mark them on the risk priority order.

Step 7: Next I have to describe also that how it can be harmful for organization and what type of damage can be came using the this.

Step 8: I have to documented all the things along with the suggestion and counter measures of it.

Question2 : Suppose you are asked to perform ARP poisoning attack. Explain the process and recommend possible countermeasures for the same.

Address Resolution Protocol (ARP) is a stateless protocol used for resolving IP addresses to machine MAC addresses. All network devices that need to communicate on the network broadcast ARP queries in the system to find out other machines' MAC addresses. ARP Poisoning is also known as **ARP Spoofing**.

Here is how ARP works −

- ARP table is needed when a machine wants to communicate with the other machine.
- The ARP-request will be broadcasted over the network is the ip address is not found in the ARP table.
- All the ip addresses of the system will be compared with the mac table by the devices connected in the network.
- If one of the machines in the network identifies this address, then it will respond to the **ARP_request** with its IP and MAC address.

What is ARP Spoofing?

ARP packets can be forged to send data to the attacker's machine.

- A large number of ARP requests and reply packets are generated to overlorded the network devices like switches
- The network device(switch) is set to forwarding mode and when the ARP Table is flooded then the device will start to act like a hub and the attacker connected with the network can catch all the packets..

The attacker uses man-in-the-Middle attack to poison the network.

ARP Poisoning − Exercise

Now I will discuss the tools required to perform the attack on the network are: -

- VMware workstation
- Kali Linux or Linux Operating system
- Ettercap Tool
- Internet connection (This attack is possible in both wired and wireless connections.)

Step1: - We must have kali Linux installed on the our virtual machine. And make sure the internet is working or not.

Step 2 − After opening the terminal type command → ifconfig

To see the ip address.

Step 4 − To perform the attack we need Ettercap as a tool installed in the system and to open the graphical interface of the toll we need to run a command → Ettercap -G

Step 5 − Now click the tab “sniff” in the menu bar and select “unified sniffing” and click OK to select the interface. We are going to use “eth0” which means Ethernet connection.

Step 6 − In the host tab go for the scan for host option then it will start scanning the whole network for the live host.

Step 7 − In the host list we have to careful full about the Ip outcome because there is a chance to have the default ip addresses there.

Step 8 − To perform the attack we need to select the target; we need to set the victim as target1 and the router as target2.

Step 9 − In this scenario, our target is Target ip and the router is router-id.

Step 10 − Now click on “MITM” and click “ARP poisoning”. Thereafter, check the option “Sniff remote connections” and click OK.

Step 12 − Now it’s time to see the results; if our victim logged into some websites. You can see the results in the toolbar of Ettercap.

This is how sniffing works. By performing the steps, I can easily get the credentials traveling through the HTTP requests

ARP Poisoning has the scope to lead an organization to a big loss and this the places the ethical hacker is needed to secure the targets.

Now how to prevent the ARP poisoning attack:

IN the section I will discuss the best possible ways to build good counter measures for it:

- We can use a good VPN service for encrypted communication to build a good and effective data communication tunnel.

- We can use static ARP entries to prevent the ARP attack with a simple way.

- **Use packet filtering**—packet filtering solutions can identify poisoned ARP packets by seeing that they contain conflicting source information, and stop them before they reach devices on your network.

- The concept of packet-filtering can be implemented in the firewall of the network. So that we can easily identify our valid packets.

- After some intervals we have to run spoofing attacks to identify if any threat is present or not.

Question 3: You have just concluded a penetration test for a client. During the test, you were able to use a phishing exploit to collect authentication credentials from several employees. To address this vulnerability, you recommend that the client conduct a mandatory security awareness training session for all employees. What type of solution is this? Explain

The Program comes under the ‘Corporate employees development plan’ and it is an important way for employers to see how vulnerable their people are to this social engineering attack and train them to do the right thing with the real thing.

The goal of a phishing simulation program is to provide employees with a safe, simulated environment where they can learn about what real phishing attempts look like in the wild.

Step1 : **Prepare your communication plan**

You should have a plan for how your simulated phishing program will flow squared away before you dive in. At the very least, this will make it easier to lay out your initiative for your executive team and specific department heads (more on that soon).

Points to cover in your communications plan should include:

- Frequency of your individual simulated phishing email campaigns (one email = one campaign)
- Supporting educational content you plan to include (articles on the company intranet, supporting graphics, etc.)
- Messaging for announcing the program companywide

- Employee-facing instructions for how to report a suspicious email

The best programs we’ve seen have common branding carried throughout their phishing educational content. Here we mean giving you’re a program a catchy name; one that your people will see and instantly associate with it. We’re fans of plays on words (something like “Paresh Phish of the Day”), but the possibilities are wide open.

A catchy name teamed with consistent colors and even font choices for your phishing communications helps engage your employee and makes clear the importance your organization places on this threat and the educational content behind it.

Step 2 : Define your methodology

Put simply, the most important thing to track is how often your phishing emails get reported; **the report rate**.

Click rates are often touted as the primary metric of simulated phishing success, but these can be too easily manipulated by tweaking the difficulty of phishing campaigns. If click rates are too low, then you’re not sending tough enough phishing emails.

Report rates help demonstrate your ultimate goal and engagement. You want people to tell you if they think they received a phishing email; simulated or not. The more they report, the more engaged your employees are.

Step 3: Make a good Contact with the Heads

Your bosses need to know what you’re doing and why. This is where you’ll be thankful you worked out a communications plan.

If your leadership is still on the fence about initiating a simulated phishing program in the first place, use data to quantify just how big of a problem phishing is and what the risk is to your organization. This can come in the form of suspicious emails blocked by your email client or malicious downloads prevented (IT will be your good friends here, as they should always be).

Step 4: Perform the Attack

Before you launch your full program, you’ll need to send a campaign without telling the company. Only your IT help desk should know.

Why all this secrecy? Keeping this first campaign under wraps is the best way to gauge your people’s everyday susceptibility to phishing emails. They won’t be expecting a test, meaning they’ll be just as vigilant (or not) as they usually are.

Establishing initial reporting percentages and click through rates is important to show how your primary simulated phishing and training initiative has improved behaviors later on.

The first simulated phishing email should not be too easy, but not too hard either. Consider something like a phony package shipping confirmation or a new voicemail announcement. The link should lead to a simple 404 page.

Step 5: Make an announcement of the program

Wait, didn't we just say the simulated phishing campaigns you're running should be secret?

Well, yes and no.

The baseline phishing email should not be public knowledge to glean as true an assessment as possible of your organization's susceptibility to phishing.

But after you get a baseline, your full, multi-month program should be formally announced to all employees.

In fact, you should over-communicate about the problem to avoid an impression that the program is a test or that you're trying to trick anyone. Communicate that the program is educational – it's part of your training and awareness efforts.

Step 6: Now Launch the Program

Here are some ideas for types of phishing campaigns to run:

- Password reset requests
- Shipping notifications around the holidays
- Requests purporting to be from HR concerning W2s around tax time (again, inform your HR director before you do this)
- Spear phising campaigns targeting specific departments or even positions (wait until at least you're three or four campaigns in, though, as spear phishing is a big jump in complexity)

Step 7: Supporting Communication

Call It awareness, no simulated phishing program is complete without supporting content outside of the emails themselves.

These can include everything from eye-catching infographic to short articles and videos posted on your company intranet. Occasional reminders to all employees about how to report phishing emails are also useful to send, interspersed with the simulated phishing emails themselves.

Last but not least, specific web pages people who click simulated phish get sent to should be educational and supportive. Again, we're not going for "gotchas" or scolding.

This content should be tied into your larger training and awareness initiative whenever possible. Try to achieve a similar look and feel to help your people mentally connect the varied training content you’ve deployed.

In all seriousness, though, a thoughtful simulated phishing program, tied to other security training and awareness elements, will pay dividends.

A program built with engagement in mind is a big step toward establishing a security culture in your organization.

An engaged employee will say something when they see something; will tell their coworkers about it.

That’s how culture spreads. And that sort of thing is priceless.

