Web pentesting ZAP

Introduction

First of all, I have used web goat for my pen testing . I have found vulnerabilities using zap and . and I also have write the code to improve this . Using which code, we can increase the security of our system and how can improve the security.

Week:1

1 Vulnerability

I have found XSS (cross site script) attack in that , SQL injection, session hijacking , password reset vulnerability, broken access control .

Vulnerability and detail

1.1 XSS

The xss attack mean cross site script . in the xss attack the user enter some milicous code in the input field or at button . when the used done some type of action then the user data get leaked if the sended code is milicous or sended by an unknown person . its simples example is <script> documents.log(“the attack”)</script> . when the user enter this in the field then a pop up came and show message written in script which is “the attack” . the above given example is too much basic . this can be more crucial.

Solution

Its solution is the validation the all inputs is verified at client side as well as at server side . if no validation is applied it can be crucial and be a cause of data leak.

1.2 SQL injection

In sql the used data can be access due to database flaw mean the data can be accessed due to database flaw . suppose when the “insert into table(name,password) values(name,pass)” when the user enter data in this table the sql command is executed . But what is the hacker enter “or “1”=1in password field then the statement will be considered that there is an “or” statement which mean one condion . and as 1=1 is true so the site will give access of the data to the hacker .

Solution

So for the prevention of this we use parametrized statements . like not direct use values . rather then we say values(?,?) and then using bind pass values which decrease the chances of being get hacked.

1.3 Session hijacking

In the session hijacking the user session is hijacked by the other person like hacer.

Session hijacking can be done using mitm and also using xss attack .

MITM in this technique a user behave as middle person between the user and the intenet . user sended data came first to the hacker and then go tho the sever and when back also came first to the hacker and then go the user .

Using xss also can be done . in this way the haker send a link to the user and then open that link the session of the user go to the hacker and the hacker can use that which is crucial.

Prevention

First of all, never click an unknow link . first verify and then click .

Second for MITM the sites use ssl certificate due to which the mitm is not now that easy .

1.5 Password reset vulnerabilities

In this when the used reset the password the password send to the user in the plain text to the mail . and if the hacker manipulate the site to send that password to the hacker mail then the password send to the hacker in the plain text form .

Prevention

To prevent this first of all not send sensitive data to the client in the plain text form . also prefer to use the mail service which is use authentication to send mail.

1.6 Broke access control

In this the user it allowed at one time then it allowed to use other account for example hacker has id=12 and then type id=14 in the link bar then the hacker can access that account due to this vulnerability

Week 2

2.1 Sanatize and validate

in sanitize and validate the user enter data should be sanitized and validated it's mean the data entered by user should we clean and clear there should not be any special symbol which can be a cause of then he attack like SQL cross site script and other

prevention

In prevention we use PHP validation so that the attacks can't be perform and can be stopped php code example

$value=filter-var($name , FILTER-VALIDATION-VAR)

The above will validate all the enterd data and validate there should be no any wrong data entered and also user trim to remove all the spaces enterd by the user .

And also store the password in the hashed form so that other if access the password this would be not too easy for that to access the hacked password .

$password=password-hash($pass,password-default)

2.2 Enhance authentication

The authentication also should be enhanced using web token . so that only validate user can access that data.

2.3 Secure header

Use helmet to secure header in my site I don’t have code so I just can explain theoretically . in this we secure the header which contain some information . which is also important . so secure this

Week 3

NMAP

We have used nmap here . using namp we can now the version of the hosting server which Is not 100% accurate but helpful

Namp 127.0.0.1 -sV

Using this we can find the which os is running

Nmap 127.0.0.1 -p-

This will scan all the top 1000 ports and tell which are open and which are closed

Namp 127.0.0.1 –script http-vuln*.

This will try to find out the vulnerability in the site server

Namp 127.0.0.1 –script http-sql-injection

This will find that there is sql possible or not

Namp 127.0.0.1 –script http-xssed

This will try to perfume xss attack

Namp 127.0.0.1 –script http-header

This will tell weather there is get or post method