B04901110 林冠宇 webgoat

1.Command Injection

/bin/sh, -c, cat "/home/robinlin/.extract/webapps/WebGoat/plugin\_extracted/plugin/CommandIn jection/resources/AccessControlMatrix.html"

if we replace AccessControlMatrix.html with

AccessControlMatrix.html” & ls # so that we can succeed in command injection.

Last but not least, we can either modify selection of AccessControlMatrix

from BurpSuite or html file of the page.

2.Numeric SQL Injection

SELECT \* FROM weather\_data WHERE station = 101 OR TRUE

and we can get every data

3.Log Spoofing

if we failed to log in, the server would write sth like

[ Login failed for username: guest ]

bur if we add sth behind guest to be

guest%0D%0A Login Succeeded for username: admin

the below would be written into log file

[ Login failed for username: guest%0D%0A Login Succeeded for username: admin]

and would be further interpreted as

[ Login failed for username: guest]

[ Login Succeeded for username: admin]

4.XPATH injection

this is very similar to SQL string injection, once we use or instead of OR

type [guest’ or ‘a’=’a] at both account and password, and we make it.

5.String SQL Injection

type [guest’ or ‘a’=’a] at both account and password, and we make it.

6. Stage 1: String SQL Injection

select the admin and then

type [guest’ or ‘a’=’a] at password, and we make it.

7. Stage 3: Numeric SQL Injection

select Larry,

and then use String SQL injection to log in as Larry

try to view profile

modify the paramater emplyee\_id at BurpSuite to be

101 or 1=1 order by employee\_id desc

and then we can view the profile of the admin which has the largest element\_id =112

8. Database Backdoors

since SQL statements are separated by ; therefore we type the following at username

[101; UPDATE employee SET salary = 20000 WHERE userid = 101]

and we can modify the salary of user 101

9. Forgot Password

just guess the user’s favorite color…. No too much to say

10. Discover Clues in the HTML

open the html file to look for comment:

in this example, a comment

<!-- FIXME admin:adminpw >

so what to do is quite obvious….