

JK Lakshmipat University Jaipur
INSTITUTE OF ENGINEERING AND TECHNOLOGY

End Term Examination, May 2019

B. Tech. in Computer Science and Engineering, Semester VI [IBM-IS and IBM-CC Batches]

Roll No.....

CSE CC601 : Application Security

Time: 3 hours

Max. Marks: 50

Instructions to students:

1. Do not write anything other than your roll number on question paper.
2. Assume suitable data wherever required and mention it clearly.
3. Writing appropriate units, nomenclature, and drawing neat sketches/schematics/ flow chart wherever, required are an integral part of the answer.
4. Calculators of any kind are NOT ALLOWED for this exam. Log Tables are NOT ALLOWED for this exam.
5. This is a CLOSED BOOK and CLOSED NOTES EXAM. That is, Notes and Books are NOT ALLOWED to be used by the students during the duration of the exam. Any Student possessing any notes, books, electronic devices etc. will be treated as a UNFAIR MEANS CASE as per university rules and is liable to be penalized as per the UNFAIR MEANS RULES followed by the University.

Q.1 Short Answer Questions: (Answer should be limited to one sentence.) 10

- i.) Mention what is the threat you are exposed to if you do not verify authorization of user for direct references to restricted resources?
- ii.) Name the attack technique that implements a user's session credential or session ID to an explicit value?
- iii.) You as a Web. Application Developer, you did not flag HTTP cookies with tokens as secure. Name the threat vector that will make your Web. Application vulnerable to attacks, with the blunder you just committed with your web application.
- iv.) Mention what happens when an application takes user inserted data and sends it to a web browser without proper validation and escaping?
- v.) What do you see as the most critical and current threats effecting Internet accessible Web Applications? (Consider the Network Security related Threats affecting web-applications also.)

Q.2 You have been asked to review the source code for a compiled script that is being used to validate logon credentials for a web application. The file is called "logon_validate" and a typical logon request looks like this – 10

"GET /cgi-bin/logon_validate?login=test&password=test"

The source code is shown below -

```
void show_error(void) {
```

```

// AUTHENTICATION ERROR

exit(-1);

}

int main(int argc, char **argv) {
char error_on_auth='1';
char user[128];
char pass[128];
char *ch_ptr_begin;
char *ch_ptr_end;

/*****/
/* Get Username from Query String */
/*****/
ch_ptr_begin=(char *)strstr(****QUERY_STRING****,"login=");
if (ch_ptr_begin==NULL)
    show_error();
ch_ptr_begin+=6;
ch_ptr_end=(char *)strstr(ch_ptr_begin,"&");
if (ch_ptr_end==NULL)
    show_error();
*(ch_ptr_end++)='\0';
strcpy(user,ch_ptr_begin);

/*****/
/* Get Password from Query String */
/*****/
ch_ptr_begin=(char *)strstr(ch_ptr_end,"password=");
if (ch_ptr_begin==NULL)
    show_error();
ch_ptr_begin+=9;
ch_ptr_end=(char *)strstr(ch_ptr_begin,"&");
if (ch_ptr_end!=NULL) *(ch_ptr_end++)='\0';
strcpy(pass,ch_ptr_begin);

if ((strcmp(user,GOOD_USER)==0) && (strcmp(pass,GOOD_PASS)==0))
error_on_auth='0';

if (error_on_auth=='0') {

    // AUTHENTICATION OK!!

} else {

    // AUTHENTICATION ERROR
    show_error();
}
}

```

```

}

// return(0); hehe could be evil ;PPPPP
exit(0);

}

```

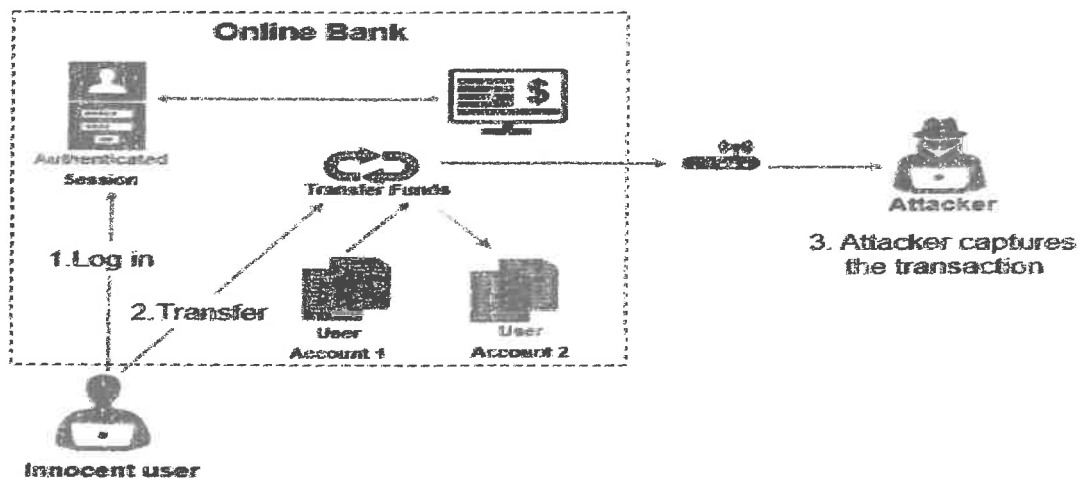
Do you see any problems with the above code? How would an attacker exploit this given code to bypass the authentication mechanisms in this program? What are some mitigation options against this type of attack?

- Q.3A You are engaged in a penetration-test where you are attempting to gain access to a protected location. You are presented with this login screen: 5



Elucidate on some of the ways/ attack vectors you will use to gain access to this protected location of the Web-Application.

- Q.3B 5

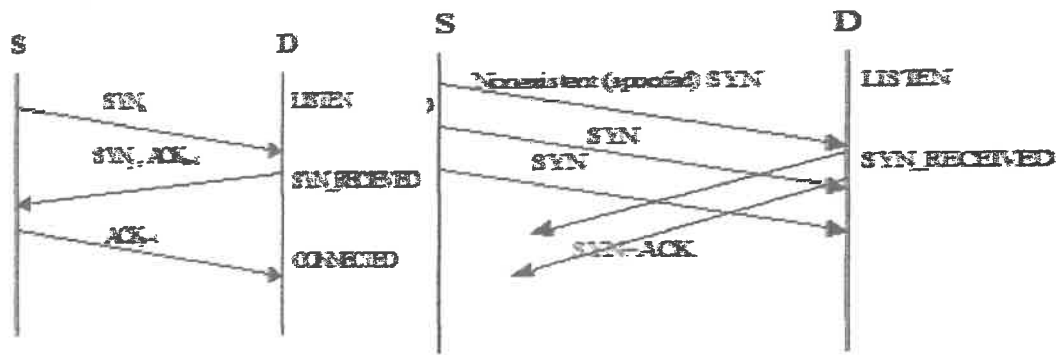


Refer to the Figure shown above, now use your knowledge, skills, intelligence and creativity to deduce like a detective the next step the attacker would take. Also, what type of attack will the attacker implement here for his/her gain or advantage? Elucidate a little bit about this attack in your own words.

- Q.4 You as a web-application penetration tester discovered a reflected XSS vulnerability where you can inject arbitrary data into a single location within the HTML of the returned page. The inserted data is truncated to 40 bytes, but you want to inject a lengthy script. You prefer not to call out to a script on an external server. How can you work around the length limit? 10

Q.5

10



Refer to the above Figure - Now Answer which network attack type is this figure pointing towards. Mention the name of the Attack and the different mechanisms through which it can be implemented. Also mention any mitigation steps for this type of attack. (Hint: The above Figure shows one of the methods through which a major network based attack can be implemented, there are many other ways to implement it also.)