STUDENT

marsak-8

TENTAMEN

2021-10-19 D0029E 0002

Kurskod	
Bedömningsform	
Starttid	19.10.2021 12:45
Sluttid	19.10.2021 16:00
Bedömningsfrist	
PDF skapad	07.09.2022 12:28

Network Security: SSL

Fråga	Status	Poäng	Uppgiftstyp	
1.1	Delvis rätt	6/10	Sammansatt	

Network Security: Authentication Protocol

Fråga	Status	Poäng	Uppgiftstyp
2.1 Fel 0/5		Flervalsfråga	
2.2	Besvarad 3/8		Essä
2.3	Delvis rätt	2/7	Flersvarsfråga

Web Security

Fråga	Status	Poäng	Uppgiftstyp
3.1	Obesvarad	0/10	Essä
3.2	Obesvarad	0/10	Essä
3.3	Rätt	10/10	Flersvarsfråga
3.4	Besvarad	10/10	Textområde

Software Security

Fråga	Status	Poäng	Uppgiftstyp
4.1	Delvis rätt	4/10	Textalternativ
4.2	Delvis rätt	7.5/15	Textalternativ
4.3	Besvarad	15/15	Essä

Multiple Choice Questions

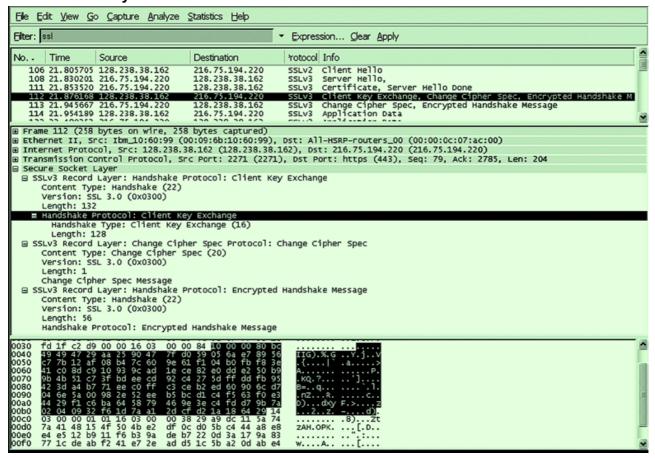
Fråga	Status	Poäng	Uppgiftstyp
5.1	Rätt	1/1	Flervalsfråga
5.2	Rätt	1/1	Flervalsfråga
5.3	Rätt	1/1	Flervalsfråga
5.4	Rätt	1/1	Flervalsfråga
5.5	Rätt	1/1	Flervalsfråga
5.6	Fel	0/1	Flervalsfråga
5.7	Rätt	1/1	Flervalsfråga
5.8	Fel	0/1	Flervalsfråga
5.9	Rätt	1/1	Flervalsfråga
5.10	Fel	0/1	Flervalsfråga
5.11	Rätt	1/1	Flervalsfråga
5.12	Rätt	1/1	Flervalsfråga
5.13	Rätt	1/1	Flervalsfråga
5.14	Rätt	1/1	Flervalsfråga
5.15	Fel	0/1	Flervalsfråga
5.16	Rätt	1/1	Flervalsfråga
5.17	Rätt	1/1	Flervalsfråga
5.18	Rätt	1/1	Flervalsfråga
5.19	Rätt	1/1	Flervalsfråga
5.20	Rätt	1/1	Flervalsfråga
5.21	Rätt	1/1	Flervalsfråga

5.22

Fråga	Status	Poäng	Uppgiftstyp
6.1	Fel	0/1	Sant/Falskt
6.2	Rätt	1/1	Sant/Falskt
6.3	Rätt	1/1	Sant/Falskt
6.4	Rätt	1/1	Sant/Falskt
6.5	Rätt	1/1	Sant/Falskt
6.6	Rätt	1/1	Sant/Falskt
6.7	Fel	0/1	Sant/Falskt
6.8	Rätt	1/1	Sant/Falskt
6.9	Rätt	1/1	Sant/Falskt
6.10	Rätt	1/1	Sant/Falskt
6.11	Rätt	1/1	Sant/Falskt
6.12	Fel	0/1	Sant/Falskt
6.13	Rätt	1/1	Sant/Falskt
6.14	Rätt	1/1	Sant/Falskt
6.15	Rätt	1/1	Sant/Falskt
6.16	Fel	0/1	Sant/Falskt
6.17	Fel	0/1	Sant/Falskt
6.18	Rätt	1/1	Sant/Falskt
6.19	Fel	113/150	Sifferfält

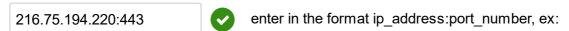
2021-10-19 D0029E 0002

1 Network Security: SSL



Consider the Wireshark output above for a portion of an SSL session. Answer the following questions

b. What is the server's IP address and port number?



192.12.123.123:8080

c. Assuming no loss and no retransmissions, what will be the sequence number of the next TCP segment sent by the client? 80 (283)

 d. Is second SSL record in message 112 part of the handshake protocol?	Candidate
O No, the handshake protocol is part of message 114	
○ Yes	
No, it is part of the change cipher spec protocol	•
There is no handshake procedure in SSL	
e. Is client authenticated in this very session? How can you prove it by analyzing exchanged messages?	the
○ Yes, because client is able to send date in message 113	
No, It does not send its certificate to server	•
○ Yes, because message 113 contains the certificate	
○ No, because message 108 forbids it to	

- Analyze the following protocol for authentication and key distribution. There X and Y are two principals, A is a key distribution center, R_X is a random number, and E_X means ncrypted with the secret key of X.
 - (1) $X \rightarrow A : X, Y, R_X$
 - (2) $A \rightarrow X : E_X(R_X, Y, K, E_Y(K,X))$
 - (3) $X \rightarrow Y : E_Y(K, X)$
 - (4) $Y \rightarrow X : E_K(R_Y)$
 - (5) $X \rightarrow Y : E_K(R_Y 1)$
- 1 What does the presence of R_X in message 2 assure?
 - Select one alternative:
 - This is a random nonce, for Diffie-Hellman key exchange.
 - This is a random nonce, which assures that the response in message 2 is for the cornitial message.
 - This is an unnecessary parameter.
 - This is a random nonce, which serves as a seed for the encryption.



Totalpoäng: 5

2 Discuss about the security aspects of the protocol. Can the protocol be made more secure, if yes, suggest methods for improving the security of this protocol?

Fill in your answer here

Right now X, Y, and R_x is shared publicly in message 1. The use of encrypted messages with the help of something like Diffey-Hellmans key exchange algorithm could make the conversation more secure.

3	What problem will be created if an attacker were to break an old K (and the attacker copied messages for that session)? Select all that is true	has also
	☐ This Protocol is a subject for reply attach from step 3 onwards.	~
	All the parameters here are static (they do not get renewed in time).	~
	Man-in-the-middle attach from step 3 onwards.	•
	This protocol is a subject for known plain text attack.	
	This protocol is sufficiently secure despite of static parameters.	
		Totalpoäng: 7

3.1 Web Security 1:

Explain what is CSRF attack, explain by giving an example attack. Also explain any two counter measures for CSRF attack. Optionally, you can add illustration to your answer (use the insert diagram option, click here to learn how to insert diagram)

Rubric used to mark your answer

- What is this attack and why is it called cross-site? (3 points)
- Description of an example attack (how would one perform such a attack) (3 points)
- Counter Measures (2 points each)

Fill in your answer here

3.2 Web Security 2:

Explain what is XSS attack, explain by giving an example attack. Also explain any two counter measures for XSS attack. Optionally, you can add illustration to your answer (use the insert diagram option, click here to learn how to insert diagram)

Rubric used to mark your answer

- What is this attack and why is it called cross-site? (3 points)
- Description of an example attack (how would one perform such a attack) (3 points)
- Counter Measures (2 points each)

Fill in your answer here

Totalpoäng: 10

3.3 Web Security 3:

Which of the following statements are false

Select one or more alternatives:

CSRF attacks are not possible for GET requests	•
☑ Both CSRF and XSS attacks happen from a third party site	•
Some GET requests need CSRF protection	
XSS attacks can be prevented by filtering user inputs	
All modern web browsers defeat XSS and CSRF attacks.	•

3.4 Web Security 4:

Assume that a database only stores the sha256 value for the *password* and *eid* columns. The following SQL statement is sent to the database, where the values of the *\$passwd* and *\$eid* variables are provided by users. Give an example input that will result in a SQL injection. If SQL injection is not possible, just say so in the answer below.

\$sql = "SELECT * FROM employee WHERE eid='SHA2(\$eid, 256)' and password='SHA2(\$passwd, 256)'";

Fill in your answer here

```
$eid = *some eid*, 256)'#
```

This problem is similar to previous problem, except that the hash value is not calculated inside the SQL statement; it is calculated in the PHP code using PHP's hash() function. Give an example input that will result in a SQL injection. If SQL injection is not possible, just say so in the answer below.

```
$hashed_eid = hash('sha256', $eid);
$hashed_passwd = hash('sha256', $passwd);
$sql = "SELECT * FROM employee WHERE eid='$hashed_eid' and
password='$hashed_passwd'";
```

Fill in your answer here

It is not possible!

Note: 5 points for each answer above.

4.1 Software Security 1:

```
In which memory segments are the variables in the following code located?
       int i = 0;
       void func(char *str)
       {
              char *ptr = malloc(sizeof(int));
              char buf[1024];
              int j;
              static int y;
        }
                                                 (Stack, BSS, Heap, Data) segment.
                           Stack
The argument str will be in
The variable y will be in BSS
                                             (Stack, Data, BSS, Heap) segment.
                                             (Stack, Data, Heap, BSS) segment.
The variable i will be in BSS
                                               (BSS, Heap, Data, Stack) segment.
The variable ptr will be in Heap
```

Totalpoäng: 10

4.2 Software Security 2:

Several students had issue with the buffer overflow attack. Their badfile was constructed properly where shell code is at the end of badfile, but when they tried, for some it worked and some did not.

buffer address: 0xbffff180

Student 1: retAddr = 0xbffff251. The attack student.	worked	~	•	(worked, did not work) for this
Student. Student 1: retAddr = 0xbffff280. The attack student.	did not work	~	8	(worked, did not work) for this
Student 1: retAddr = 0xbffff300. The attack student.	did not work	~	•	(worked, did not work) for this
Student 1: retAddr = 0xbffff310. The attack student.	did not work	~	*	(did not work, wroked) for this
Student 1: retAddr = 0xbffff400. The attack	did not work	~	⊘	(did not work, worked) for this
student.				

4.3 Software Security 3:

The following function is called in a privileged program. The argument str points to a string that is entirely provided by users (the size of the string is up to 300 bytes). When this function is invoked, the address of the buffer array is 0xAABB0010, while the return address is stored in 0xAABB0050. Please write down the string that you would feed into the program, so when this string is copied to buffer and when the bof() function returns, the privileged program will run your code. In your answer, you don't need to write down the injected code, but the offsets of the key elements in your string need to be correct.

Fill in your answer here

Buffer array address: oxAABBoo10

Return pointer address: oxAABBoo50

Offset: 40

The distance between return address and the buffer is 64. I have put my shell code at 256 bytes from the beginning of the buffer. Hence I have selected AABBo266 as my return address.

```
index o - 63 will have NOPs
index 64 - 68 will have the return address AABB0266
index 69 - 255 will have NOP
index 256 to end of the buffer will have shell code.
```

Note: there are 8 bits in 1 byte and 0xAABB0050 is 4 bytes in length

Example Answer:

The distance between return address and the buffer is 32. I have put my shell code at xxx bytes from the beginning of the buffer. Hence I have selected 0xABCD1234 as my return address.

```
Index 0 - 31 will have NOP (x90) index 32 - 35 will have the return address ABCD1234 index 36 - xxx - 1 will have NOP(x90)
```

index xxx to end of the buffer will have shell code.

		Totalpoäng: 15
5.1	The most common means of human-to-human identification are Select one alternative:	
	facial characteristics	•
	○ fingerprints	
	○ signatures	
	○ retinal patterns	
		Totalpoäng: 1
5.2	systems identify features of the hand, including shape, and lengths a fingers. Select one alternative: Palm Print	and widths of
	Hand geometry	•
	○ Signature	
	○ Fingerprint	
		Totalpoäng: 1

5.3	Each individual who is to be inclined in the system. Select one alternative:	uded in the database of authorized users must first be
	identified	
	verified	
	enrolled	
	authenticated	
		Totalpoäng: 1
5.4	To counter threats to remote user authentication, systems generally rely on some form of protocol. Select one alternative:	
	denial-of-service	
	challenge-response	
	○ trojan horse	
	eavesdropping	
		Totalpoäng: 1

5.5	The is what the virus "does".	
	Select one alternative:	
	○ trigger	
	infection mechanism	
	O logic bomb	
	payload	•
		Totalpoäng: 1
5.6	The is when the virus function is performed. Select one alternative:	
	opropagation phase	
	triggering phase	✓
	O dormant phase	
	execution phase	×
		Totalpoäng: 1
5.7	During the the virus is idle. Select one alternative:	
	○ triggering phase	
	o dormant phase	•
	execution phase	
	opropagation phase	
		Totalpoäng: 1

16/29

5.8	A uses macro or scripting code, typically embedded in a documer when the document is viewed or edited, to run and replicate itself into other suc Select one alternative:	
	file infector	
	multipartite virus	~
	O boot sector infector	
	macro virus	×
		Totalpoäng: 1
5.9	is the first function in the propagation phase for a network worm. Select one alternative:	
	Propagating	
	 Spear phising 	
	○ Keylogging	
	Fingerprinting	•
		Totalnoäng: 1

lotalpoang: 1

5.10	The Packet Storm Web site includes a large collection of packaged shellcode, including code that can: Select one alternative:		
	set up a listening service to launch a remote shell when connected to	~	
	create a reverse shell that connects back to the hacker		
	flush firewall rules that currently block other attacks		
	all the above	×	
	Tota	alpoäng: 1	
5.11		. •	
5.11	aim to prevent or detect buffer overflows by instrumenting programs when are compiled.	. •	
5.11	aim to prevent or detect buffer overflows by instrumenting programs when are compiled. Select one alternative:	. •	
5.11	aim to prevent or detect buffer overflows by instrumenting programs when are compiled. Select one alternative: Compile-time defenses	. •	
5.11	aim to prevent or detect buffer overflows by instrumenting programs when are compiled. Select one alternative: Compile-time defenses Shellcodes	. •	
5.11	aim to prevent or detect buffer overflows by instrumenting programs when are compiled. Select one alternative: Compile-time defenses Shellcodes Run-time defenses	. •	

5.12	can prevent buffer overflow attacks, typically of global data, which attempt to overwrite adjacent regions in the processes address space, such as the global offset table.		
	Select one alternative:		
	○ MMUs		
	 Guard pages 	•	
	○ Heaps		
	All the above		
	То	otalpoäng: 1	
5.13	is a form of overflow attack. Select one alternative:		
	Heap overflows		
	Return to system call		
	Replacement stack frame		
	All the above	•	
	Т	otalpoäng: 1	

5.14	The used a buffer overflow ex	ploit in "fingerd" as one of its attack mechanisms.
	Select one alternative:	
	Morris Internet Worm	
	Slammer Worm	
	Sasser Worm	
	○ Code Red Worm	
		Totalpoäng: 1
5.15	A attack occurs when the input subsequently executed by the system with	is used in the construction of a command that is the privileges of the Web server.
	Select one alternative:	
	O PHP remote code injection	✓
	command injection	×
	○ SQL injection	
	ovirus injection	
		Totalpoäng: 1

5.16	A attack is where the input includes code that is then executed by the attacked system.
	Select one alternative:
	○ cross-site scripting
	code injection
	○ SQL injection
	interpreter injection
	Totalpoäng:
5.17	Blocking assignment of form field values to global variables is one of the defenses available to prevent a attack.
	Select one alternative:
	ocommand injection
	○ SQL injection
	mail injection
	PHP remote code injection
	Totalpoäng:

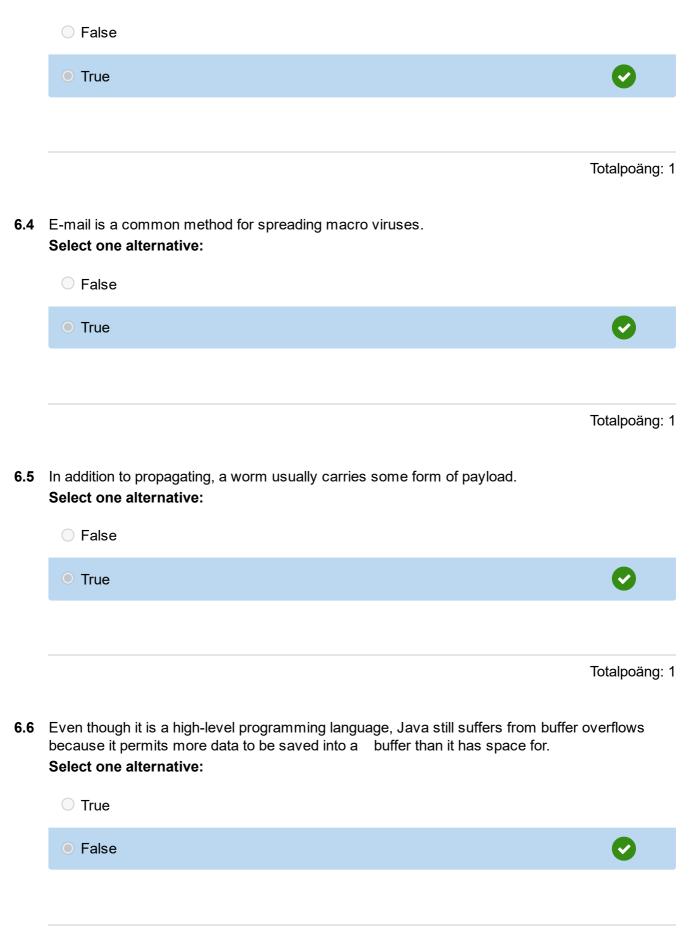
5.18	attacks are vulnerabilities involving the incontent of a Web page displayed by a user's browser.	clusion of script code in the HTML
	Select one alternative:	
	O PHP file inclusion	
	Code injection	
	Cross-site scripting	
	Mail injection	
		Totalpoäng: 1
5.19	A is a pattern composed of a sequence of c variants.	haracters that describe allowable input
	Select one alternative:	
	○ race condition	
	regular expression	
	○ shell script	
	canonicalization	
		Totalpoäng: 1

5.20	The most complex part of TLS is the		
	Select one alternative:		
	○ signature		
	handshake protocol		
	O payload		
	message header		
		Totalpoäng: 1	
5.21	is the process in which a CA issues a certificate for a user's public key and returns that certificate to the user's client system and/or posts that certificate in a repository. Select one alternative:		
	 Registration 		
	Initialization		
	Certification		
	Authorization		
		Totalpoäng: 1	

5.22	is the process whereby a user first makes itself known to a CA prior to that CA issuing a certificate or certificates for that user.
	Select one alternative:
	 Certification
	 Authorization
	Registration
	 Initialization
	Totalpoäng: 1
6.1	A logic bomb is the event or condition that determines when the payload is activated or delivered Select one alternative:
	○ True
	False
	Totalpoäng: 1
6.2	Many forms of infection can be blocked by denying normal users the right to modify programs on the system. Select one alternative:
	○ True
	○ False
	Totalpoäng: 1

6.3 A macro virus infects executable portions of code.

Select one alternative:



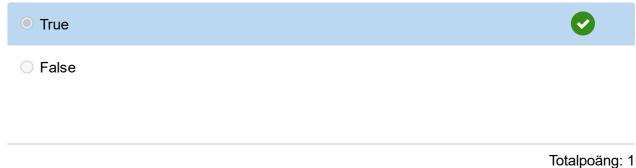
6.7 Stack buffer overflow attacks were first seen in the Aleph One Worm.

Select one alternative:



6.8 A stack overflow can result in some form of a denial-of-service attack on a system.

Select one alternative:



6.9 An attacker is more interested in transferring control to a location and code of the attacker's choosing rather than immediately crashing the program.

Select one alternative:

False True



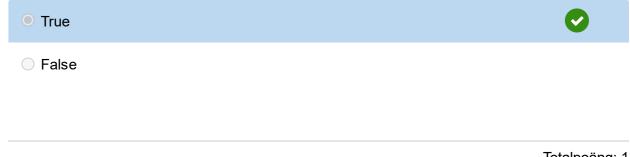
6.10 The potential for a buffer overflow exists anywhere that data is copied or merged into a buffer, where at least some of the data are read from outside the program.

Select one alternative:



6.11 Defensive programming requires a changed mindset to traditional programming practices.

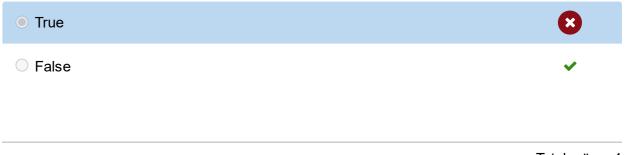
Select one alternative:



Totalpoäng: 1

6.12 To counter XSS attacks a defensive programmer needs to explicitly identify any assumptions as to the form of input and to verify that any input data conform to those assumptions before any use of the data.

Select one alternative:



6.13 Injection attacks variants can occur whenever one program invokes the services of another program, service, or function and passes to it externally sourced, potentially untrusted information without sufficient inspection and validation of it.

Select one alternative:

	○ False	
	True	•
	To	otalpoäng: 1
6.14	Cross-site scripting attacks attempt to bypass the browser's security checks to gair access privileges to sensitive data belonging to another site. Select one alternative:	n elevated
	○ False	
	True	•
	To	otalpoäng: 1
6.15	To prevent XSS attacks any user supplied input should be examined and any danger removed or escaped to block its execution. Select one alternative:	rous code
	True	•
	○ False	

6.16 The ticket-granting ticket is encrypted with a secret key known only to the AS and the TGS. Select one alternative: True False Totalpoäng: 1 The ticket-granting ticket is not reusable. 6.17 Select one alternative: False True Totalpoäng: 1 **6.18** Kerberos does not support interrealm authentication. Select one alternative: True False Totalpoäng: 1 **6.19** How many points did you get for Dugga 1? Enter the points from Canvas. **(1514356)** 113 Totalpoäng: 150