Final exam in

Web Security EITF05

Department of Electrical and Information Technology
Lund University

November 2nd, 2018, 14.00–19.00

- You may answer in either Swedish or English.
- If any data is lacking, make (and state) reasonable assumptions.
- Use legible hand writing. If your answers cannot be read, you will receive zero points on that problem.
- Grading is done as follows.
  Grade 3 = 20–29 points,
  Grade 4 = 30–39 points,
  Grade 5 = 40–50 points.

Good luck!

Paul

Problem 1. Consider an SQL injection attack.

a) Write some PHP code and use it to illustrate and explain how an SQL injection attack works.

b) Motivate why this is potentially the most dangerous attack for any company.

c) How does the same origin policy protect against SQL injection attacks? (3 points)

Problem 2. Give a regular expression that matches an IP address (IPv4). The following variations should match;

```
127.0.0.1
255.255.255.255
0.0.0.0
```

but not

```
256.256.256.256
123.456.789.012
```

Matching leading zeros is optional. (3 points)

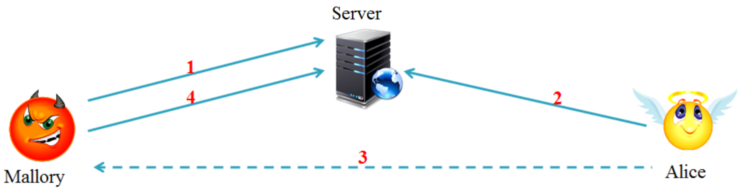
Problem 3. Consider a DNS server that implements Domain Name System Security Extensions (DNSSEC).

a) How many signatures does the DNS server need to generate on-the-fly for each DNS request it receives? Motivate.

b) NSEC allows zone walking. What is zone walking, and how (explain the idea briefly) is this prevented in NSEC3?

(1.5+1.5 points)

Problem 4. Consider the following illustration of an XSS attack with three involved entities; Mallory, Server and Alice.



a) Does TLS protect against XSS attacks? Motivate.

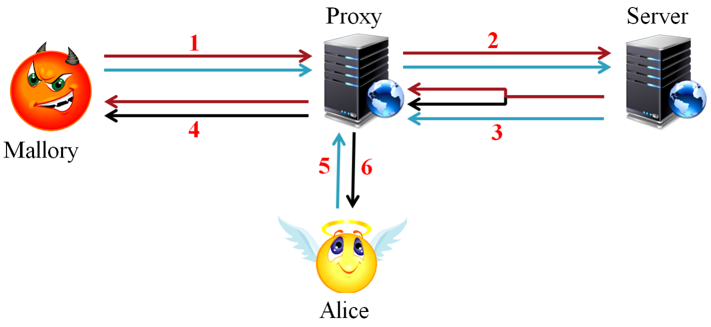
b) What provides good protection against XSS attacks? Motivate.

(1.5+1.5 points)

Problem 5. Explain how Domain-based Message Authentication, Reporting and Conformance (DMARC) works.

(3 points)

Problem 6. Consider the following illustration of an HTTP response splitting attack.



a) Briefly explain how an HTTP response splitting attack works. You may refer to the picture.

b) In the attack, what is the purpose of the Proxy?

(2+1 points)

Problem 7. A DKIM signature header of an email is given below.

```
DKIM-Signature:
v=1;
a=rsa-sha256;
c=simple/relaxed;
d=gmail.com;
s=gamma;
h=received:message-id:date:from:to:subject:mime-version:content-type;
bh=9gicsZnlcLK7yYh6VIrgyAMMRZiWsSbWqSPIhc78RRk=;
b=k4ofvpHPkaQmvuSoGVhRrnCsPK+JEuv9KUrZO7aiypvf/6Y1N2iIatvLvdzwOnZX
  /W6Kxyx6Z4Ybuk8Dqk/vNTIE7Jpy+GQUUHFvMONFtmZo1CbGRvo8DdHnXRBB/qWw
  lV+Z6wxw/mq7lNuJknVprOAaTLws5mwcZ+AWL8KwHgO=
```

a) Does DKIM support usage of more than one public key per domain? Motivate.

b) How does DKIM provide integrity protection, and for which parts of the email? (What is signed, and how?)

(1.5+1.5 points)

Problem 8. An engineers has censored some famous quotes using Base64. What did they say? Choose any **one**. Show your calculation.

Margaret Atwood, The Blind Assassin:
The best way of `a2VlcGluZw==` a secret is to pretend there isn't one.

George Orwell, 1984:
If you want to keep a secret, you must also hide it from `eW91cnNlbGY=`.

Benjamin Franklin, Poor Richard's Almanack:
Three may keep a secret, if two of them are `ZGVhZA==`.

Hint: Decimal representation of ASCII characters:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122

The Base64 alphabet:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
0	1	2	3	4	5	6	7	8	9	+	/														
52	53	54	55	56	57	58	59	60	61	62	63														

(3 points)

Problem 9. Bitcoin uses a hasing technique that is very similar in functionality to that used in Hashcash. Consider a Hashcash solution in which a string

$$ver : bits : date : resource : rand : counter$$

is hashed using SHA-1, where

ver is version number (currently 1),
bits indicates how costly the function is for sender,
date gives current date,
resource is recipients email address,
rand is a random number.

a) How is a proper *counter* value determined?

b) How many times must the hash function be invoked to *generate* a valid Hashcash header with $bits = 30$? Exactly or on average?

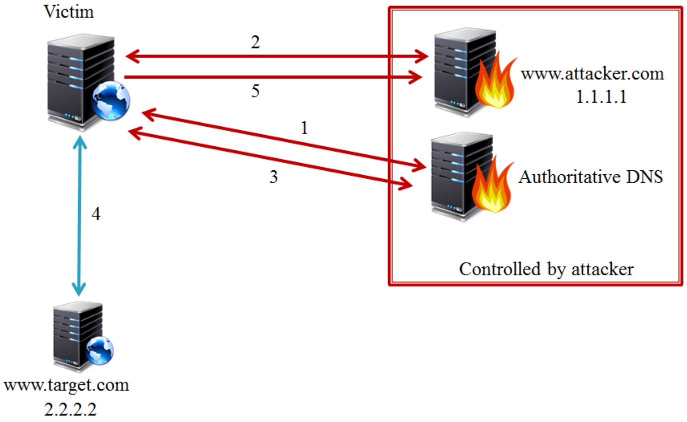
c) How many times must the hash function be invoked to *verify* a valid Hashcash header with $bits = 30$? Exactly or on average?

(3 points)

Problem 10. Consider the following illustration of a DNS rebinding attack.

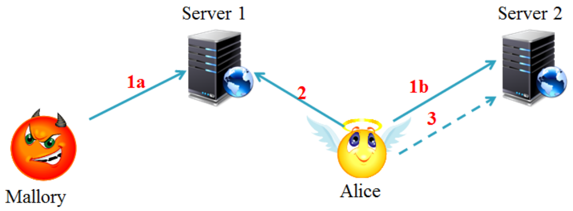
a) Will the attack work if there is a firewall between the Victim and the Attacker? Motivate.

b) How would step 3 differ if the Victim's browser implements DNS-pinning?



(1.5+1.5 points)

Problem 11. Consider the following illustration of a CSRF attack.



a) Briefly explain how a CSRF attack works. You may refer to the picture.

b) Explain how CSRF protection with synchronizer token pattern works.

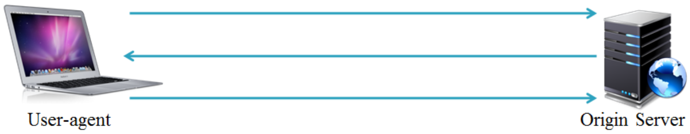
(2+3 points)

Problem 12. HTTP digest authentication (RFC2617) is a challenge response protocol in which the client calculates the digest (the response) according to

$$\mathrm{MD5}(\ \mathrm{MD5}(A1) : \mathit{nonce} : \mathit{nc} : \mathit{cnonce} : \mathit{qop} : \mathrm{MD5}(A2)\ ),$$

with

$$\begin{aligned} A1 &= \mathit{username} : \mathit{realm} : \mathit{password}, \\ A2 &= \begin{cases} \mathit{method} : \mathit{URI} & \text{if } \mathit{qop} = \mathit{auth}, \\ \mathit{method} : \mathit{URI} : \mathrm{MD5}(\mathit{entity\text{-}body}) & \text{if } \mathit{qop} = \mathit{auth\text{-}int}. \end{cases} \end{aligned}$$



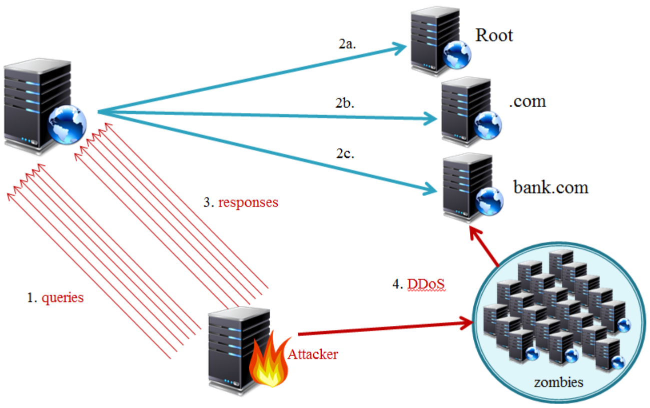
a) Explain the usage and purpose of the *realm* parameter?

b) Why does the *cnonce* parameter protect against TMTO attacks?

c) The *nonce* parameter does not protect against TMTO attacks, why?

(1+2+2 points)

Problem 13. Consider the following illustration of a DNS cache poisoning attack. The success rate of the attack depends on how many queries and responses that can be sent in steps 1 and 3 (before the first response in step 2c has been delivered).



a) How is the birthday paradox leveraged in the DNS cache poisoning attack?

b) What is the purpose of the botnet?

c) How would usage of TCP (instead of UDP) provide protection? Motivate.

(2+1+2 points)

Problem 14. Briefly explain the following terms and acronyms.

a) SMTP

b) Reflected XSS

c) CORS

d) Digest HTTP authentication

e) HEAD (the HTTP method)

(5 points)
