Université de Boumerdes UMBB
Faculté des Sciences
Sécurité Informatique
RIAHLA Med Amine

Série N° 4 : Vulnérabilités des réseaux

Exercice 1 «CSS/XSS et Injection SQL »

1. Qu'est ce qu'une attaque par CSS/XSS ?
2. Quelle précaution doit-on prendre pour éviter une attaque cross site Scripting?
3. Qu'est ce qu'une attaque par injection SQL ?
4. Quelle est la différence fondamentale entre le cross site Scripting (CSS) et l'injection SQL ?

BankCustomer est une banque qui donne la possibilité à ses clients d'accéder à leurs comptes bancaires via un site internet. Pour cela, le client saisie son nom d'utilisateur (login) et son mot de passe (password) via un formulaire et attend que le serveur lui donne accès à son compte. La requête SQL pour interroger le serveur de base de données telle qu'elle est implémenté par le concepteur du site est la suivantes : (par exemple pour un login=user et un password=psswd) :

```
SELECT nom, pw FROM database WHERE nom = "user" AND password = "psswd"
```

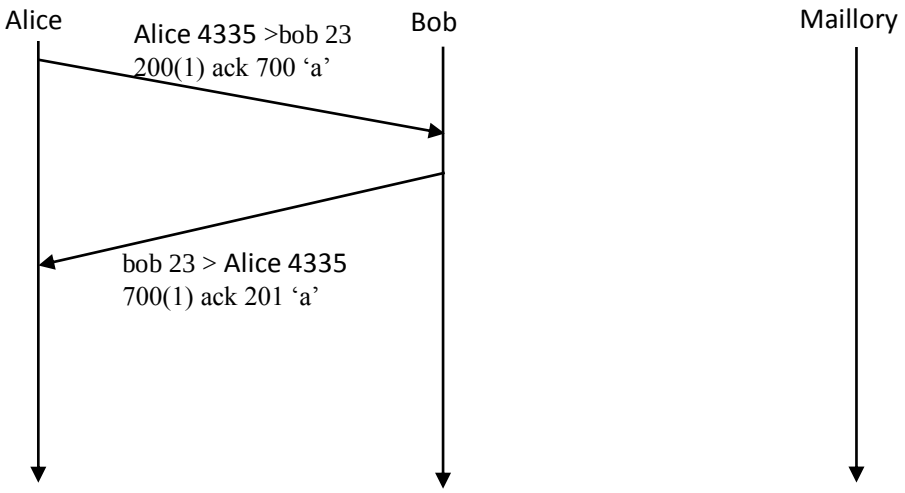
5. Donner deux méthodes qui permettent à un pirate d'accéder aux données du SGBD de la banque sans avoir un login et un passsword valides.

6. Que doit faire l'administrateur du site pour régler ce problème?

Exercice 2 « Vol de session TCP »

UN PIRATE (Maillory) espionne une connexion telnet. Il forge un paquet TCP pour insérer la commande \n echo hacked \n dans le flux de données. Le dernier échange de paquets avant l`insertion est illustré à la figure suivante.

Compléter cette figure avec le paquet inséré et les paquets suivants.



Exercice 3 « Attaque de Kevin Mitnick »

Le trafic décrit ci-dessous à été observé dans un réseau (cas réel). De quoi s'agit-il ?
Les paquets TCP sont décrits à l'aide de lignes ayant le format suivant :

14 :18 : 37.26 Alice.513>bob.514 : P 1382727010(2) ack 2024384001

On y trouve :

- L'heure (14 :18 :37 .26)
- L'adresse source (Alice)
- Le port source(513)
- L'adresse destination (bob)
- Le port destination(514)
- Un flag éventuel (S=syn, p=push, F =fin, R=reset, .=pas de flag)
- Le numéro de séquence du premier octet de données transmise dans ce paquet (1382727010)
- Le numéro d'octet transmis(2)
- Un éventuel acquittement des octets reçus (ack)
- Le numéro de séquence du prochain octet attendu(2024384001).

14:18:22.51	mallory.600 > alice.513:	S	1382726960	
14:18:22.56	mallory.601 > alice.513:	S	1382726961	
14:18:22.74	mallory.602 > alice.513:	S	1382726962	
14:18:22.83	mallory.603 > alice.513:	S	1382726963	
14:18:22.88	mallory.604 > alice.513:	S	1382726964	
14:18:22.94	mallory.605 > alice.513:	S	1382726965	
14:18:23.00	mallory.606 > alice.513:	S	1382726966	
14:18:23.10	mallory.607 > alice.513:	S	1382726967	
14:18:23.16	mallory.608 > alice.513:	S	1382726968	
14:18:23.22	mallory.609 > alice.513:	S	1382726969	
14:18:23.28	mallory.610 > alice.513:	S	1382726970	
14:18:23.34	mallory.611 > alice.513:	S	1382726971	
14:18:23.40	mallory.612 > alice.513:	S	1382726972	
14:18:23.90	mallory.613 > alice.513:	S	1382726973	
14:18:24.00	mallory.614 > alice.513:	S	1382726974	
14:18:24.08	mallory.615 > alice.513:	S	1382726975	
14:18:24.14	mallory.616 > alice.513:	S	1382726976	
14:18:24.20	mallory.617 > alice.513:	S	1382726977	
…	**…**	**…**	**…**	
14:18:25.90	kevin.1000 > bob.514:	S	1382726990	
14:18:26.09	bob.514 > kevin.1000:	S	2021824000	ack 1382726991
14:18:26.17	kevin.1000 > bob.514:	R	1382726991	
14:18:26.50	kevin.999 > bob.514:	S	1382726991	
14:18:26.69	bob.514 > kevin.999:	S	2021952000	ack 1382726992
14:18:26.77	kevin.999 > bob.514:	R	1382726992	
14:18:27.01	kevin.998 > bob.514:	S	1382726992	
14:18:27.17	bob.514 > kevin.998:	S	2022080000	ack 1382726993
14:18:27.25	kevin.998 > bob.514:	R	1382726993	
14:18:27.54	kevin.997 > bob.514:	S	1382726993	
14:18:27.71	bob.514 > kevin.997:	S	2022208000	ack 1382726994
14:18:27.79	kevin.997 > bob.514:	R	1382726994	
14:18:28.05	kevin.996 > bob.514:	S	1382726994	
14:18:28.22	bob.514 > kevin.996:	S	2022336000	ack 1382726995
14:18:28.30	kevin.996 > bob.514:	R	1382726995	
14:18:28.56	kevin.995 > bob.514:	S	1382726995	
14:18:28.73	bob.514 > kevin.995:	S	2022464000	ack 1382726996
14:18:28.81	kevin.995 > bob.514:	R	1382726996	
14:18:29.07	kevin.994 > bob.514:	S	1382726996	
14:18:29.27	bob.514 > kevin.994:	S	2022592000	ack 1382726997

```
14:18:29.35   kevin.994 > bob.514:    R   1382726997
14:18:29.58   kevin.993 > bob.514:    S   1382726997
14:18:29.75   bob.514 > kevin.993:    S   2022720000   ack 1382726998
14:18:29.84   kevin.993 > bob.514:    R   1382726998
14:18:30.09   kevin.992 > bob.514:    S   1382726998
14:18:30.26   bob.514 > kevin.992:    S   2022848000   ack 1382726999
14:18:30.34   kevin.992 > bob.514:    R   1382726999
14:18:30.60   kevin.991 > bob.514:    S   1382726999
14:18:30.77   bob.514 > kevin.991:    S   2022976000   ack 1382727000
14:18:30.85   kevin.991 > bob.514:    R   1382727000
14:18:31.11   kevin.990 > bob.514:    S   1382727000
14:18:31.28   bob.514 > kevin.990:    S   2023104000   ack 1382727001
14:18:31.36   kevin.990 > bob.514:    R   1382727001
14:18:31.62   kevin.989 > bob.514:    S   1382727001
14:18:31.79   bob.514 > kevin.989:    S   2023232000   ack 1382727002
14:18:31.87   kevin.989 > bob.514:    R   1382727002
14:18:32.16   kevin.988 > bob.514:    S   1382727002
14:18:32.33   bob.514 > kevin.988:    S   2023360000   ack 1382727003
14:18:32.41   kevin.988 > bob.514:    R   1382727003
14:18:32.67   kevin.987 > bob.514:    S   1382727003
14:18:32.84   bob.514 > kevin.987:    S   2023488000   ack 1382727004
14:18:32.92   kevin.987 > bob.514:    R   1382727004
14:18:33.18   kevin.986 > bob.514:    S   1382727004
14:18:33.35   bob.514 > kevin.986:    S   2023616000   ack 1382727005
14:18:33.43   kevin.986 > bob.514:    R   1382727005
14:18:33.69   kevin.985 > bob.514:    S   1382727005
14:18:33.98   bob.514 > kevin.985:    S   2023744000   ack 1382727006
14:18:34.06   kevin.985 > bob.514:    R   1382727006
14:18:34.20   kevin.984 > bob.514:    S   1382727006
14:18:34.37   bob.514 > kevin.984:    S   2023872000   ack 1382727007
14:18:34.45   kevin.984 > bob.514:    R   1382727007
14:18:34.71   kevin.983 > bob.514:    S   1382727007
14:18:34.88   bob.514 > kevin.983:    S   2024000000   ack 1382727008
14:18:34.96   kevin.983 > bob.514:    R   1382727008
14:18:35.22   kevin.982 > bob.514:    S   1382727008
14:18:35.39   bob.514 > kevin.982:    S   2024128000   ack 1382727009
14:18:35.47   kevin.982 > bob.514:    R   1382727009
14:18:35.73   kevin.981 > bob.514:    S   1382727009
14:18:35.90   bob.514 > kevin.981:    S   2024256000   ack 1382727010
14:18:35.98   kevin.981 > bob.514:    R   1382727010
14:18:36.24   alice.513 > bob.514:    S   1382727010
14:18:36.75   alice.513 > bob.514:    .                ack 2024384001
14:18:37.26   alice.513 > bob.514:    P   1382727010(2) ack 2024384001
14:18:37.77   alice.513 > bob.514:    P   1382727012(5) ack 2024384001
14:18:38.28   alice.513 > bob.514:    P   1382727017(25) ack 2024384001
14:18:41.34   alice.513 > bob.514:    .                ack 2024384002
14:18:42.25   alice.513 > bob.514:    .                ack 2024384003
14:18:43.16   alice.513 > bob.514:    F   1382727042   ack 2024384003
14:18:52.17   alice.513 > bob.514:    R   1382727043
14:18:52.23   alice.513 > bob.514:    R   1382727044
14:18:52.29   mallory.600 > alice.513:  R   1382726960
14:18:52.36   mallory.601 > alice.513:  R   1382726961
14:18:52.41   mallory.602 > alice.513:  R   1382726962
14:18:52.47   mallory.603 > alice.513:  R   1382726963
14:18:52.53   mallory.604 > alice.513:  R   1382726964
14:18:52.60   mallory.605 > alice.513:  R   1382726965
14:18:52.66   mallory.606 > alice.513:  R   1382726966
14:18:52.71   mallory.607 > alice.513:  R   1382726967
14:18:52.77   mallory.608 > alice.513:  R   1382726968
14:18:52.83   mallory.609 > alice.513:  R   1382726969
14:18:52.93   mallory.610 > alice.513:  R   1382726970
14:18:52.99   mallory.611 > alice.513:  R   1382726971
14:18:53.05   mallory.612 > alice.513:  R   1382726972
14:18:53.11   mallory.613 > alice.513:  R   1382726973
```

Exercice 4 « TCP/IP spoofing»

On rappelle que l`IP spoofing consiste pour un pirate à se faire passer pour une machine B auprès d`une machine A (au niveau de l'adressage IP). L'attaque se compose généralement de trois étapes :

- Le pirate paralyse la machine B.
- Le pirate devine le procédé utilisé par A pour générer ses numéros de séquence initiaux (ISN).
- Le pirate se fait passer pour B auprès de A.

1- Que se passerait-il si le pirate ne paralysait pas la machine B ?
2-Pourquoi est-il nécessaire de déterminer la manière dont A génère ses ISN ?
3-Quel peut être l'intérêt pour le pirate de se faire passer pour la machine B ?

Exercice 5 « Trafic réseau suspect »

Conrad ministrateur. Un informaticien qui travaille pour une banque suisse .est responsable du bon fonctionnement et de la sécurité du réseau de son employeur. Un matin, lors d'un contrôle de routine, il remarque du trafic suspect à destination de serveur qui gère la base de données des comptes bancaires des clients un extrait de ce trafic est sur la figure ci-dessous.

```
02:01:27 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:27 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:27 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
```

Sachant que l'adresse 192.168 .94.1 est celle de la passerelle qui offre un accès à internet à ce serveur, interpréter ce trafic de manier concise.