P. Lafourcade, C. Olivier-Anclin, M. Puys

TP5 – Attaques Web

Préparation : cela peut prendre un peu de temps, commencez le reste du TP en parallèle.

- Dans VDN, téléchargez l'image docker suivante : `https://sancy.iut.uca.fr/~lafourcade/SECU-3A/lab7.tar.gz`
- Entrez la commande suivante : `docker load -i lab5.tar.gz`
- Entrez la commande suivante : `docker run --rm --add-host=host.docker.internal:host-gateway -p 5000:5000 lab5`
  La commande tourne en continu, laissez le terminal tel quel.

Exercise 1 (Shodan et NMAP (3 points))
Si shodan n'est pas accessible depuis l'IUT, testez depuis chez vous.

1. Rendez-vous sur la page `https://www.shodan.io/domain/uca.fr` et balayez la liste des résultats. A quoi correspond cette page ? Reconnaissez-vous des domaines connus ?
2. Repérez la machine correspondant à `codefirst.iut.uca.fr`. Quelle est son adresse IP ? Quels ports sont ouvert dessus ?
3. Rendez-vous sur la page `https://www.shodan.io/host/45.33.32.156` et balayez la liste des résultats. A quoi correspond cette page ? Quels services tournent sur la machine en question ? Sont-ils vulnérables ?

Attention : tout scan informatique non autorisé est assimilable à une attaque informatique et peut être répréhensible selon la loi française. Les scans fait lors de ce TP se limiteront aux machines de la salle de TP et à la machine distante `scanme.nmap.org`.

Lancez toutes les commandes nmap avec l'option -T4 pour accélérer l'exécutions.

4. Effectuez un scan "PING" des hôtes présents dans la salle de TP. Quelle commande avez-vous utilisé ? Expliquez les résultats.

Effectuez la suite des manipulations liées à NMAP dans VDN pour avoir les droits administrateur.

5. Effectuez un scan "SYN TCP" et "UDP" sur une machine de la salle de TP. Quelle commande avez-vous utilisé ? Expliquez les résultats.
6. Effectuez un scan permettant la détection des OS et des versions sur une machine de la salle de TP. Quelle commande avez-vous utilisé ? Expliquez les résultats.

Exercise 2 (Failles XSS (2 points))

1. Donner la définition d'une attaque attaque XSS réfléchie. Puis Accédez à la page suivante : `http://127.0.0.1:5000` et réalisez une attaque XSS réfléchie. Comment avez-vous fait ?
2. Donner la définition d'une attaque attaque XSS stockée. Puis accédez à la page suivante : `http://127.0.0.1:5000` et réalisez une attaque XSS stockée. Comment avez-vous fait ?

Exercise 3 (Failles LFI et RFI (3 points))
Sur la page web, nettoyez les commentaires existants s'il y en a avec le bouton "Clear" de la page web. Le code Python permettant le filtrage des commentaires par le serveur est le suivant :

```
def get_comments(search_query=None):
    db = connect_db()
    results = []
    get_all_query = 'SELECT comment FROM comments'
    for (comment,) in db.cursor().execute(get_all_query).fetchall():
        if search_query is None or search_query in comment:
            results.append(comment)

    if search_query and results == []:
        if search_query.endswith(".pyb"):
            results = [execute(search_query)]
        elif search_query.startswith("http"):
            results = [requests.get(search_query).text]
        else:
            try:
                results = [open(search_query, "rb").read()]
            except FileNotFoundError:
                pass

    return results
```

1. Réalisez une attaque LFI sur le fichier /etc/shadow du serveur web. Comment avez-vous fait ? Expliquez la vulnérabilité dans le code. Trouvez le mot de passe du compte root du serveur avec john ou équivalent.

2. Réalisez une attaque RFI incluant la page `http://perdu.com`. Comment avez-vous fait ? Expliquez la vulnérabilité dans le code. Essayez avec d'autres pages web.

3. Réalisez une attaque RFI exécutant la page

   `https://sancy.iut.uca.fr/~lafourcade/SECWEB/attack.pyb`.

   Comment avez-vous fait ? Expliquez la vulnérabilité dans le code.

Exercise 4 (SQL Injection (6 points))
L'objectif est de trouver des attaques SQL à la main dans un premier temps sur une base de données et dans un second temps de se servir des outils `SQLMAP`[1], `JohnTheRipper`[2] et `HashCat`[3] pour hacker une autre base de données.

Télécharger le fichier suivant avec:

```
wget https://sancy.iut.uca.fr/~lafourcade/SECU-3A/SQLIA.tar
```

Pour lancer docker aller dans le répertoire `SQLIA` et faites `docker-compose up` ce qui va lancer le site `http://172.19.19.19:8080/`.

Tester que le site est accessible avec `links http://172.19.19.19:8080` en ligne de commande (ou avec Firefox), ou bien `curl http://172.19.19.19:8080/`

Il faut peut-être `unset` le proxy et/ou utiliser `links`.

Une fois docker quitté il faut faire `docker-compose down --volumes` pour arrêter proprement le système.

[1] `https://sqlmap.org/`
[2] `https://www.openwall.com/john/`
[3] `https://hashcat.net/wiki/doku.php?id=example_hashes`

1. Aller sur la page `level0` et monter une attaque par SQL injection sur le site `myblog.com` pour se connecter comme `user` et comme `admin`. Sachant que la requête à la base de données est :

   ```
   SELECT * FROM users
   WHERE ‘email‘ = ’" . $email . "’ AND ‘password‘ = ’" . $password . "’";
   ```

   Quand le nombre de résultats de la requête est 1 alors l'utilisateur choisi peut se connecter.

2. Installer SQLMAP en faisant un git clone de :

   ```
   https://github.com/sqlmapproject/sqlmap.git --depth=1 --single-branch --branch 1.5.9
   ```

   Aller sur la page `level1` et utiliser l'outil `SQLMAP` avec les options `--data` et ensuite `--dump` (cette deuxième option est lente mais très efficace). Pour récuperer la totalité de la BD.

   Une fois le contenu de la BD obtenu, utiliser le dictionnaire `rockyou.txt` disponible à

   ```
   https://perso.limos.fr/~gamarcadet/enseignement/websec23/rockyou.txt.tar.gz
   ```

   avec le logciel JohnTheRipper ou Hashcat pour retoruver les mots de passe des deux utilisateurs de ce niveau.

Remarque pour effeacer les résultats de `sqlmap` il faut faire `sqlmap --purge`.

Exercise 5 (Failles CSRF (6 points))

1. Télécharger le fichier suivant : `https://sancy.iut.uca.fr/~lafourcade/SECU-3A/CSRF_bad_server.tar` Placez ce fichier dans votre `public_html` ou bien lancez le serveur avec la commande `php`. Authentifiez-vous sur le site avec le login `etudiant` et le mot de passe `securepassword`. Validez que vous pouvez afficher et modifier le mot de passe. Attention, si votre session PHP est détruite, le mot de passe redeviendra celui par défaut.

2. Quels champ de formulaire pouvez-vous trouver dans le formulaire de changement de mot de passe ?

3. Regardez le code du serveur et notez qu'il ne présente aucune protection contre les attaques par CSRF. Créez une page `malicious.html` qui permet de modifier le mot de passe en `motdepasspirate` une fois le client authentifié.

4. Proposez une correction du code du serveur implémentant une protection à base de token CSRF aléatoires et vérifiez que votre page d'attaque ne fonctionne plus.