2013/2014

M2-Informatique SSI

GULDNER Geoffrey
HURIER Médéric
LACAVE Valentin
SOIHILI Mouchtali

[Rapport d'Echec Attaque]

SOMMAIRE

I. Echec Attaque n°EA001

Type d'attaque
Scanner de vulnérabilité web (Nikto)

Groupe visé
Groupe 2

Description de l'attaque
Lancement du scanner avec les options par défaut
nikto -h 172.24.141.119
nikto -h 172.24.141.124

Objectif de l'attaque
Détection de vulnérabilité sur les applications des autres groupes.

Cause de l'échec de l'attaque
Le site ne suit pas un fonctionnement standard. Les pages non trouvées (code 404) sont indiquées comme des pages trouvées par le navigateur (code 200). Le scanner croît alors que toutes les pages qu'il recherche existent, alors que ce n'est pas le cas.

II. Echec Attaque n°EA002

Type d'attaque
Scanner de vulnérabilité web (Nikto)

Groupe visé
Groupe 3

Description de l'attaque
Lancement du scanner avec les options par défaut
nikto -h 172.24.141.125
nikto -h 172.24.141.211

Objectif de l'attaque
Détection de vulnérabilité sur les applications des autres groupes.

Cause de l'échec de l'attaque
Aucune faille critique n'a été révélée.

III. Echec Attaque n°EA003

Type d'attaque
Scanner NESSUS

Groupe visé
Groupe 2

Description de l'attaque
Le but de cette attaque était de trouvée des vulnérabilités sur leur serveur pour pouvoir les exploiter plus tard.

Objectif de l'attaque
Détection de vulnérabilité sur les servers.

Cause de l'échec de l'attaque
Echec du scanner du au port bloquée ou au système de défense qui a pu être mis en place.

IV. Echec Attaque n°EA004

Type d'attaque
Scanner NESSUS

Groupe visé
Groupe 3

Description de l'attaque
Le but de cette attaque était de trouvée des vulnérabilités sur leur serveur pour pouvoir les exploiter plus tard.

Objectif de l'attaque
Détection de vulnérabilité sur les servers.

Cause de l'échec de l'attaque
Echec du scanner du au système de défense qui a pu être mis en place.

V. Echec Attaque n°EA005

Type d'attaque
Scanner SQLMap

Groupe visé
Groupe 3

Description de l'attaque
Le but de cette attaque était de trouvée des vulnérabilités sur leur application web pour effectuer des injections SQL pour pouvoir les exploiter plus tard.

Objectif de l'attaque
Détection de vulnérabilité SQL

Cause de l'échec de l'attaque
Echec du scanner du au système de défense qui a pu être mis en place et au port bloquée. (Mais détection de la tentative de scanner par GOLRT)

VI. Echec Attaque n°EA006

Type d'attaque
Scanner SQLMap

Groupe visé
Groupe 2

Description de l'attaque
Le but de cette attaque était de trouvée des vulnérabilités sur leur application web pour effectuer des injections SQL pour pouvoir les exploiter plus tard.

Objectif de l'attaque
Détection de vulnérabilité SQL

Cause de l'échec de l'attaque
Echec du scanner du au système de défense qui a pu être mis en place et au port bloquée.

VII. Echec Attaque n°EA007

Type d'attaque
Injection sql

Groupe visé
Groupe 2

Description de l'attaque
1er essai : On fait sauter les défenses coté client avec firefox (clic droit examiner l'élément et on modifie le code)
On essaye une injection sql sur le champ de login du groupe 2

2eme essai : On créé un article avec un nom de titre contenant une injection sql et on l'upload

Objectif de l'attaque
Obtenir des informations confidentielles genre user, mots de passes,… .

Cause de l'échec de l'attaque
Les injections SQL sont filtrées, et les caractères spéciaux remplacés.

VIII. Echec Attaque n°EA008

Type d'attaque
Injection sql

Groupe visé
Groupe 3

Description de l'attaque
1er essai : On fait sauter les défenses coté client avec firefox (clic droit examiner l'élément et on modifie le code)
On essaye une injection sql sur le champ de login du groupe 3

2eme essai : On créé un article avec un nom de titre contenant une injection sql et on l'upload

3eme essai : On regarde le code de la page et on remarque un bouton d'upload pour les articles avec un champ 'id' ou similaire, on remplace la valeur cachée du bouton par une injection SQL.

Objectif de l'attaque
Obtenir des informations confidentielles genre user, mots de passes,… .

Cause de l'échec de l'attaque
Les injections SQL ne sont filtrées mais ils utilisent des classes SQL qui font qu'on ne peut rien obtenir (construction d'objets).

IX. Echec Attaque n°EA009

Type d'attaque
Injection XSS

Groupe visé
Groupe 2

Description de l'attaque
On créé un article avec des balises spéciales dans le but de faire des injections XSS et on les upload sur le serveur du groupe 2.

Objectif de l'attaque
Faire tourner du code autre que celui prévu par les clients ou le serveur.

Cause de l'échec de l'attaque
Les articles sont entre des balises <noscript> </noscript>

X. Echec Attaque n°EA010

Type d'attaque
Injection XSS

Groupe visé
Groupe 3

Description de l'attaque
On créé un article avec des balises spéciales dans le but de faire des injections XSS et on les upload sur le serveur du groupe 3.

Objectif de l'attaque
Faire tourner du code autre que celui prévu par les clients ou le serveur.

Cause de l'échec de l'attaque
Les articles sont entre des balises <noscript> </noscript>