|  |  |
| --- | --- |
| Numéro de série | {report\_number} |
| Date | {report\_date} |

**{target\_host}**

**Rapport sur la détection floue de l'API de la plate-forme**

Version 1.2

12/2020

© 2020 Packer FuzzeR Team

Poc-Sir、KpLi0rn、Liucy、RachesseHS、Lupin-III

* **Avis de droit d'auteur**

Le modèle de rapport d'inspection de Packer Fuzzer (ci-après dénommé « le présent rapport ») est protégé par les droits d'auteur de l'équipe de développement de Packer Fuzzer (ci-après dénommée « l'équipe ») et est protégé par la loi. L'équipe a le droit de modifier et d'interpréter ce modèle de rapport. Lorsque vous modifiez le contenu de ce modèle de rapport, vous devez conserver la mention de copyright appropriée. L'outil Packer Fuzzer (ci-après dénommé « l'outil ») ne peut être utilisé de quelque manière que ce soit à des fins commerciales sans l'autorisation de cette équipe. L'équipe se réserve le droit de poursuivre la responsabilité légale de toute personne ou société qui enfreindrait la déclaration ci-dessus.

* **Déclarations d'application**

Ce rapport s'applique à tous les systèmes cibles testés avec cet outil, il faut donc le garder en sécurité et ne pas le transmettre sans l'autorisation du propriétaire du système cible.

* **Clause de non-responsabilité**

Ce rapport est généré automatiquement par l'outil sur la base des résultats des tests de l'utilisateur, et le contenu du rapport ne représente pas la position et l'opinion de notre équipe. Toutes les conséquences et pertes directes ou indirectes causées par la diffusion ou l'utilisation des fonctions de test fournies par cet outil sont de la responsabilité de l'utilisateur, et l'équipe n'en assume pas la responsabilité. Veuillez respecter les lois et réglementations locales de l'utilisateur et du pays où se trouve le système cible lorsque vous utilisez cet outil, tout test non autorisé est interdit.

* **Révision des dossiers**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N° de Ver | Date de révision | Modificateur | Record de modifi | Ratifiant |
| 1.0 | 2020/8/5 | RachesseHS | / | Poc-Sir |
| 1.2 | 2020/12/18 | RachesseHS | Add More | Poc-Sir |

**I. Résumé du rapport**

**Plateformes scannées : {target\_host}**

Valeurs des paramètres d'entrée.：{target\_url}

Cette analyse utilise {scan\_type} comme mode de balayage，utilise {scan\_ip} Comme scan IP，temps total passé : {scan\_time} seconde.

Le temps d'initialisation du balayage：{start\_time}

Le temps d'achèvement du balayage：{end\_time}

Le scan a trouvé {api\_num} interfaces API valides.

Total trouvé {js\_num} dossiers JS connexes，respectivement：

{js\_list}

Total trouvé {vuln\_num} vulnérabilités de sécurité, dont {vuln\_h\_num} risque élevé、{vuln\_m\_num} risque moyen、{vuln\_l\_num} faible risque。respectivement：

{vuln\_list}

Informations supplémentaires sur les cookies : {extra\_cookies}

Informations supplémentaires de l'en-tête de transmission：{extra\_head}

**L'analyse de cet outil a montré que la plate-forme cible présente un niveau de risque de sécurité：{sec\_lv}**

**II. Détails sur la vulnérabilité**

{vuln\_deta}

**III. Liste des API**

{api\_list}

**IV. Recommandations en sécurité**

{suggest\_foryou}

**V. Informations additionnelles**

extra

**VI. Annexes**

* **Description de la vulnérabilité**

**Vulnérabilité du CORS：**Le partage de ressources entre domaines peut assouplir la politique d'homologie du navigateur, permettant à différents sites web et différents serveurs de communiquer entre eux par le biais du navigateur. Supposons qu'un utilisateur se connecte à vuln.com, un site web contenant une configuration CORS, et qu'il accède également à evil.com, un lien fourni par l'attaquant. Le site web de evil.com demande à vuln.com des données sensibles, et la capacité du navigateur à recevoir ces informations dépend de la configuration de vuln.com. Si vuln.com est configuré avec l'en-tête Access-Control-Allow-Origin et qu'il est attendu, il est alors autorisé à le recevoir, sinon le navigateur ne le recevra pas en raison de la même politique d'origine.

**Vulnérabilité à l'accès non autorisé：**Un accès non autorisé à l'interface, comme son nom l'indique, peut accéder directement aux fonctions de logique commerciale correspondantes et les exploiter sans demander d'autorisation. Cela est généralement dû à une page d'authentification défectueuse ou non authentifiée, à une mauvaise configuration de la sécurité, etc.

**Vulnérabilité des informations sensibles：**La fuite d'informations désigne la divulgation d'informations sensibles dans une page de site web ou un fichier JS. Grâce à ces informations sensibles, un attaquant peut compromettre davantage le serveur.

**Failles horizontales des ultra vires：**On parle de vulnérabilité par saut lorsqu'une application ne vérifie pas strictement les autorisations d'identité des opérations de l'utilisateur actuel, ce qui permet à un utilisateur d'exploiter des fonctions qui dépassent ses privilèges administratifs, et donc d'exécuter certaines actions qui ne sont pas disponibles pour cet utilisateur. La neutralisation des niveaux peut permettre aux utilisateurs d'un même niveau d'accéder aux informations sensibles des autres utilisateurs, telles que le nom, le numéro de téléphone, l'adresse de contact, les données personnelles, l'historique des commandes, etc. Il peut également être possible d'exécuter une série de fonctions, telles que supprimer, ajouter, modifier, etc., comme d'autres utilisateurs ayant des privilèges de dépassement de niveau.

**Vulnérabilité de l'injection SQL：**La vulnérabilité d'injection SQL survient parce que l'application web est écrite sans validation des données soumises au serveur par l'utilisateur (type, longueur, validité des paramètres commerciaux, etc.), et sans filtrage efficace des caractères spéciaux des données saisies par l'utilisateur, de sorte que l'utilisateur saisit directement dans l'exécution de la base de données, au-delà des résultats attendus de la conception originale de l'instruction SQL, ce qui entraîne une vulnérabilité d'injection SQL.

**Vulnérabilité des mots de passe faible：**En raison d'une sensibilisation insuffisante à la sécurité, le personnel de gestion et d'exploitation du site web utilise des mots de passe très faciles à retenir ou adopte directement le mot de passe par défaut du système par souci de commodité et pour éviter d'oublier les mots de passe. Les attaquants peuvent utiliser cette vulnérabilité pour entrer directement dans le système d'application ou le système de gestion, de manière à altérer et supprimer le système, les pages web, les données, accéder illégalement au système, aux données des utilisateurs, et peuvent même entraîner la chute du serveur.

**Vulnérabilité au téléchargement arbitraire de fichiers：**Le système d'application vérifie la validité du type de fichier, du format et du contenu du fichier téléchargé par l'utilisateur lors de la fonction de téléchargement de fichiers, qui permet aux attaquants de télécharger des scripts malveillants à partir du Shell Web (.php, .jsp, .asp, etc.) ou des fichiers dans des formats non prévus tels que les fichiers HTML, SHTML, etc. à un répertoire web ou à tout autre répertoire, ce qui peut entraîner l'exécution de fichiers de script malveillants arbitraires sur un serveur distant pour accéder directement au système d'application.

* **Niveaux de vulnérabilité**

Ce rapport comporte trois niveaux de vulnérabilité intégrés, qui sont : un risque faible, moyen et élevé. Les types de vulnérabilité à haut risque sont : vulnérabilité faible des mots de passe, vulnérabilité du téléchargement arbitraire de fichiers, vulnérabilité de l'injection SQL ; les types de vulnérabilité à risque moyen sont : vulnérabilité du saut horizontal, vulnérabilité de la divulgation d'informations sensibles, vulnérabilité de l'accès non autorisé ; les types de vulnérabilité à faible risque sont : vulnérabilité CORS.

Le niveau de confiance pour le « faible » niveau des résultats de détection réduira automatiquement la vulnérabilité d'un niveau de dommage, si celui-ci est au plus bas niveau de vulnérabilité n'est pas un déclassement. Par exemple, une vulnérabilité pour : la vulnérabilité d'injection SQL, devrait être une vulnérabilité à haut risque, mais le niveau de confiance est « faible », il est automatiquement déclassé au risque de vulnérabilité.

* **Niveau du risque**

Dans ce rapport, il existe quatre niveaux de risque : aucun risque, risque faible, risque moyen et risque élevé, et le score correspondant est respectivement de 0, 5, 10 et 18. Par exemple, dans une certaine analyse, une vulnérabilité à haut risque, cinq vulnérabilités à faible risque et deux vulnérabilités à risque moyen sont trouvées, le score est calculé comme suit : 1 x 6 + 2 x 2 + 5 x 1 = 15 (points), le score est supérieur à 15 et inférieur à 18, le niveau de risque est donc « risque moyen ».

**（Conclusion du rapport, avec les blancs suivants）**