Directory Traversal

1-تعريفها: هي ببساطة مش ثغرة ولكن تكنيك بنستخدمه مع ثغرات تانية عشان نوصل لهدفنا, ببساطة احنا بنكون في مسار محدد وعايزين نخرج منه فبنستخدم الـ Path traversal عشان نخرج من المسار الحالي ونروح للمسار الي احنا عايزينه.

- الـ path Traversal دايماً بتكون موجودة مع الـ LFI لما بنوصل إننا محتاجين نـ include ملف معين ولكن احنا مش ف نفس مساره ف بنستخدم الـ Path Traversal عشان نخرج من المسار الحالي ونروح للمسار الي فيه الملف الي عايزين نعمله include.
- الصور دايما بتتخزن في مسار var/www/images ف لما يكون في بارامیتر بالشكل ده filepath=205.png ده معناه إنه دخل على المسار الي فوق ده.

2-أسباب حدوثها:

- السبب الوحيد للثغرة دي هو إن التطبيق يستدعي صورة/ملف من السيرفر بدون ما يكون في أي قيود على البارامیتر ده, زي مثلا www.example.com/test.php?imagepath=205.png هنا هو بيجيب صورة ولكن سهل جدا على الـ Attacker إنه يتلاعب بالبارامیتر ده.
- زي ما قولنا إن الصورة ليها مسار معين وبالتالي لو عايزين نستغل الرابط الي فوق ده ونوصل لملف الباسوردات الي في موجود على السيرفر، هنعمل الاتي /../../../etc/passwd.. كده هو هيرجع 3 خطوات لورا من المسار الحالي وبالتالي هيكون في مسار الـ root والي فيه كل الملفات المهمة من ضمنهم ملف etc/ والي بداخله ملف الـ passwd وبيحمل كل باسوردات اليوزرز الي على السيرفر (بس الـ passwords بتكون encrypted).

3-ازاي تلاقيها:

- من خلال طريقتين:

❖ 1- Input Vector Enumeration: وده معناه إنك بتدور على كل input موجود وكل file upload وكل حاجة بتقبل من الـ user إنه يدخل content, وبتسأل كام سؤال مهم يساعدوك:

هل في بارامیتر في الريكوست ممكن نستخدمه في عمليات خاصة بالملفات؟

هل في Extention File غريب؟

كمان ممكن تركز في الكوكيز الي بتعمل إنشاء لتمبلت أو صفحة.

❖ 2- Automatic method: ودي عن طريق الـ Command line tools, أو عن طريق الـ scanners زي الـ Burpsuite.

4-تستغلها ازاي:

- أول حاجة هي إنك تقرأ ملفات حساسة زي /etc/passwd او ملف الـ config مثلا ودول بعض الحاجات المهمة:
- الـ /proc/version : بتظهرلك الـ version بتاع اللينكس ولو version قديم تشوف exploit ليه.
- الـ /proc/mounts : ده ملف في List للمفات الموجودة ف الsystem والي من خلاله تشوف انت عايز ايه.
-

5-بعض طرق الـ Bypass:

- 1- تجرب المسار ع طول بدون /.. , يعني تجرب /etc/passwd بس. (absolute path)
- 2-أحيانا بنلجأ اننا نستخدم // مزدوج, وبالتالي البايلود هيكون ....//....//....//(stripped non-recursively)
- 3- لو الي فوق منجحش يبقى تعمل encoding للـ / وبعدين double encoding URL.
- 4-لو التطبيق بيعمل validate للبارامتر عن طريق إنه بيجبرك تبدأ بمسار ملف معروف زي كده /var/www/images ف هتكمل من بعدها عادي جدا كل بايلود جربناه فوق.
- 5- لو بيعمل validate إن لازم يكون آخر المسار .png أو .pdf. وكده ف استخدم الـ null byte وبعده الـ .png أو الـ .pdf. وغيرهم.
- 6- تحاول تفتح الملف بـ file://etc/passwd
- 7- تشيل اسم الملف وتشوف لو ممكن يظهر أسماء باقي الملفات الي موجودة كمثال:

www.example.com/index.php?page=style.php

ف تخليه www.example.com/index.php?page= وتشوف هيظهر حاجة ولا لا.

- هنا أنت بتجرب الي فوق والي موجودين هنا LFI-Bypass وتشوف التطبيق بيتعامل معاهم ازاي وبعدين تظبط البايلود بتاعك على حسب هو بيعمل بلوك لإيه وبيعدي إيه، ف الموضوع مش static وتحفظهم وخلاص.

6-تمنع الثغرة ازاي؟:

- عشان تمنع الثغرة دي لازم تـ validate الـ Input عشان اليوزر ميتحكمش فيه ويروح لمسار مختلف وحساس.
- يكون عندك whitelist بالملفات الي ممكن تعملها include عشان لو الـ Attacker حاول يعمل include لملف مش موجود ف الـ whitelist مش هيتعمله Include.

Local File Inclusion

1-تعريفها: هي ثغرة بتسمح للمهاجم إنه يـ include file معين من الـ Web server عن طريق الـ Web browser, وخطورتها لما الـ Attacker يفكر يـ include sensitive file زي مثلا /etc/passwd أو لما يرفع شيل وبعدين يعمله include وبالتالي الكود الي في صفحة الشيل كمثال (shell.php) هيتم تنفيذه (في حالة path traversal مش هيحصل تنفيذ ولكن تقدر تقرأ بس) وهنا مثال للـ inscure code :-

```
<?php
include_file = $_GET['stylecode'] #Get file
include($include_file)) # include file
?>
```

2-أسباب حدوثها:

- السبب الرئيسي الي بيسبب ثغرة LFI هي الـ Function المسئولة عن إدراج ملف - Include - وهما كالآتي:

✔ include()

✔ include_once()

✔ require()

✔ require_once()

- محتاج تعرف الـ Functions دي وإنها المسئولة عن الثغرة عشان لو معاك source code لموقع معين انت بتيست عليه ف تشوف الـ Functions دي وتشوف هي Vulnerable ولا لا.

3-ازاي تلاقيها:

- زيها زي Path traversal وهو إنك بتشوف أي User Input بيقبل file ف تجرب فيه ثغرة الـ LFI.
- أحيانا بيكون مش كاتب امتداد الصفحة يعني مش كاتب language= en.php وبالتالي هو بيكون مكتوب language= en وهكذا او صورة مثلا ورقمها 650 ف الـ URL المفروض هتشوفه كده image=650.jpg ولكن هو بيظهر كده image=650 أو ممكن يغير اسم البارامتر أصلا وميكونش Image او أي حاجة سهلة.
- ف ممكن تستخدم الـ Burp suite وهي هتجيب الثغرات بقى واسمها بيكون path traversal في البرب.

#-ملاحظة:

- ثغرة الـ LFD = Local File Disclosure هي نفس تعريف وفكرة وازاي تلاقي ثغرة الـ LFI ولكن الاختلاف إن ثغرة LFI لما بتيجي تـ include file بيحصل تنفيذ لكود الصفحة دي بينما الـ LFD بيعرض المحتوى بس وبقدر اشوف الكود نفسه.

4-تحويلات للثغرة:

- بتحول الـ LFI لـ LFD وده عن طريق:

✔ الـ Wrapper file:// وده بدل ما تكتب /etc/passwd/ بتكتب file://etc/passwd.

✔ الـ Wrapper expect:// ولكن ده by deafult في اللغة مش enabled.

✔ الـ php://filter/convert.base64-encode/resource=file.php وبالتالي هو هيعمل encode للسورس كود لملف الـ file.php ف مش هيتنفذ وبعدين اعمل decode واقرأ السورس كود, يبقى ده مهم عشان يعمل encode for source code عشان الصفحة متفهمهوش وبالتالي مش هتنفذه.

- تاني طريقة إنك تحولها لـ RCE وده عن طريق:
- صفحات الـ File Upload وهو إنك بترفع شيل ولو عرفت توصل لمكانه بتعمله include.
- عن طريق الـ PHP Session (شرحها آخر حاجة لوحدها)

- عن طريق الـ php://input وتبعت POST داتا (الميثود هتكون POST والداتا هتكون الـ php code الي عايز تنفذه)
- عن طريق الـ Log Files ودي files موجودة في أي web server (بالاخص apache) والملفات دي انا اقدر أكتب فيها بما إنها بتسجل أي حاجة بعملها كيوزر، وبالتالي لو انا كتبت ف الـ input كود php كده انا اقدر include الـ file ده وبالتالي هيتنفذ ويتنفذ معاه الـ PHP code الي انا كتبته ومن ضمن الملفات دي:

✔ /var/log/apache2/access.log/

✔ /var/log/apache2/error.log/

✔ /Var/log/sshd.log

✔ /var/log/mail

- عن طريق ملف الـ proc/self/environ

#-ملاحظة:

- لما بنستخدم الـ PHP كـ لغة ف إنها تـ create sessions وتـ handle الموضوع هي, ف كل يوزر بيكون ليه session id فيه معلومات عنه واليوزر نيم بتاعه وهكذا وده بيتحفظ جوا مسار معين ولنفترض هو var/lib/php/sess_[php_Session]d وبالتالي لو انا بدلت الـ session id (المعلومات الي جوا زي اليوزر نيم أو على حسب هي بتخزن إيه) بـ - shell code هيتحفظ جوا ملف الsession في المسار الي فوق ف لو عملتله include هيحصله excute.

#-مقالات:

- https://medium.com/@Aptive/local-file-inclusion-lfi-web-application-penetration-testing-cc9dc8dd3601

- https://www.hackingarticles.in/smtp-log-poisioning-through-lfi-to-remote-code-exceution/
- Local/Remote file inclusion, LFD, and Path Traversal شرح ثغرات -41 دي أهم مصدر.