الفصل السادس عشر
ثغرة ال Path Traversal

المؤلف
د.م/ أحمد هاشم الفقي
استشارى أمن المعلومات و التحول الرقمي
Ahmed.Hashem.ElFiky@outlook.com

ثغرة ال Path Traversal

- عدم استخدام طرق للتحقق من دخل المستخدم الغير مسموح به يمكن أن يؤدي إلى استغلال النظام ويتيح لمختبر الاختراق قراءة وكتابة الملفات الغير مصرح له بالوصول إليها وعندها يمكنه تنفيذ كود خبيث على السيرفر أو تنفيذ تعليمات على النظام الهدف.
- سيرفرات الويب وتطبيقات الويب تستخدم طريقة للمصادقة من أجل التحكم بالوصول إلى الملفات والمصادر.
- سيرفر الويب يحاول تخصيص مساحة لكل مستخدم وكل مستخدم يمكنه الوصول فقط للمساحة المخصصة له لرفع ملفات تطبيق الويب الخاص به.
- تعريف الصلاحيات يتم من خلال قائمة التحكم بالوصول (Access Control Lists (ACL والتي تحدد أي مستخدمين أو أي مجموعات مسموح لهم بالوصول والتعديل على الملفات في السيرفر.

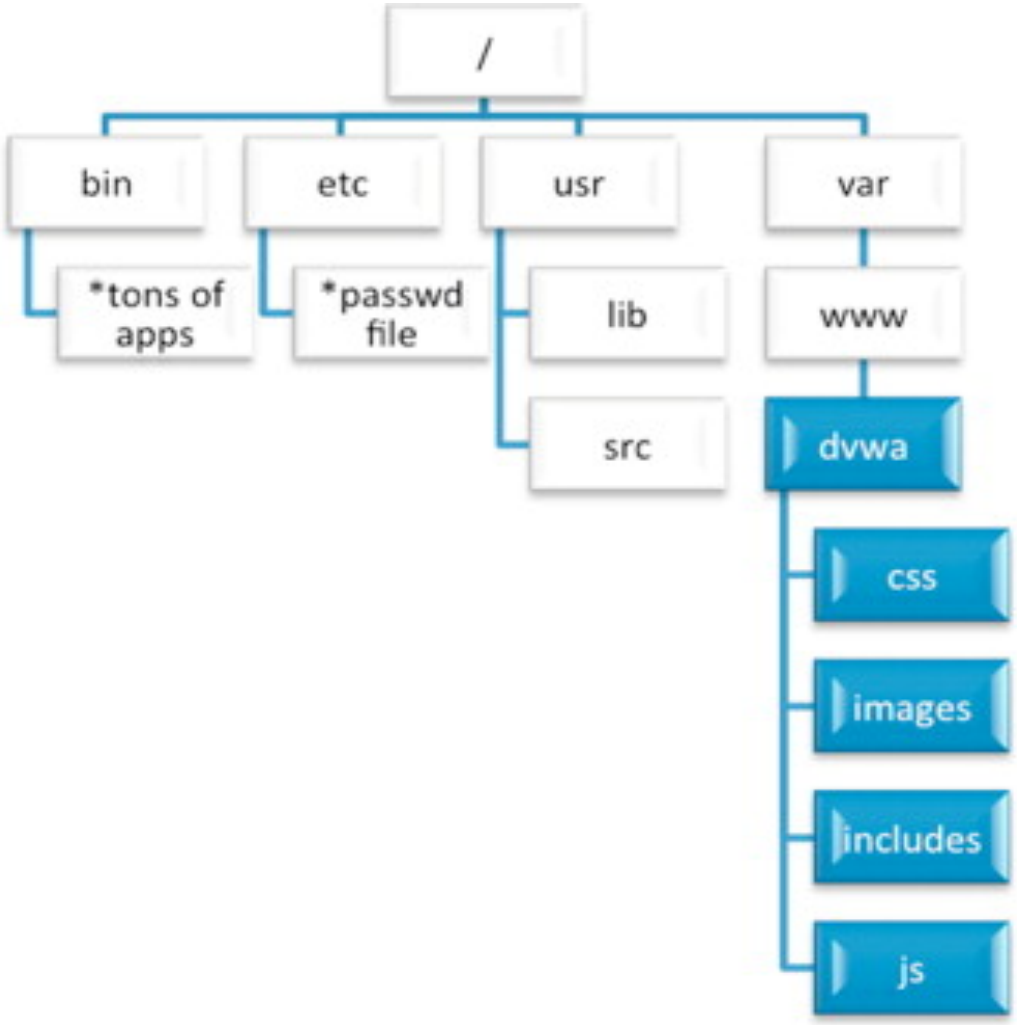
ثغرة ال Path Traversal (تكمله...)

- هذه الطريقة مُعدة لتقوم بمنع المستخدم الخبيث من الوصول إلى الملفات التي تحوي على معلومات حساسة مثل الملف (/etc/passwd) ولمنعه من تنفيذ تعليمات على النظام.
- تطبيق الويب يمكن أن يكشف معلومات حساسة إذا لم يتم التحقق من برامترات الدخل بشكل جيد.
- في هجموم تجاوز المسار path traversal في سيرفرات وتطبيقات الويب فإن مختبر الاختراق يكون قادر على قراءة الملفات والمجلدات الغير مصرح له بالوصول إليها (موجودة خارج المساحة المخصصة لتطبيق الويب)
- هذا الهجوم يعرف باسم dot-dot-slash attack (../) أو باسم backtrackingويحدث هذا الهجوم عندما يحاول مختبر الاختراق إبطال مفعول أي إجراءات حماية ومصادقة قام بوضعها مدير التطبيق ومبرمج التطبيق للسماح لمستخدمي التطبيق بالوصول فقط إلى مجلدات معينة دون مجلدات أخرى.

ثغرة ال Path Traversal (تكمله...)

- هذا النوع من الهجوم يتم عادتاً من قبل مستخدم قام بعملية المصادقة في التطبيق ويقوم بفحص المصادر التي يمكن للمستخدم العادي الوصول إليها ثم يقوم بخلق طلب خبيث لاستخدامه بالوصول إلى المصادر الغير مصرح له بالوصول إليها.
- بنية ملفات سيرفر الويب:
- في هذا المثال نستخدم سيرفر يعمل بنظام التشغيل لينكس والتطبيق الهدف هو DVWA فإن بنية المجلدات ستكون كما في الشكل التالي:

ثغرة ال Path Traversal (تكمله...)



المجلدات ذات اللون الأزرق هي المجلدات التي يس مح تطبيق الويب للمستخدم بالوصول إليها، وكل المجلدات ذات اللون الأبيض لا يسمح لمستخدمي تطبيق الويب الوصول إليها وهي مخصصة فقط لمدير السيرفر.

ثغرة ال Path Traversal (تكمله...)

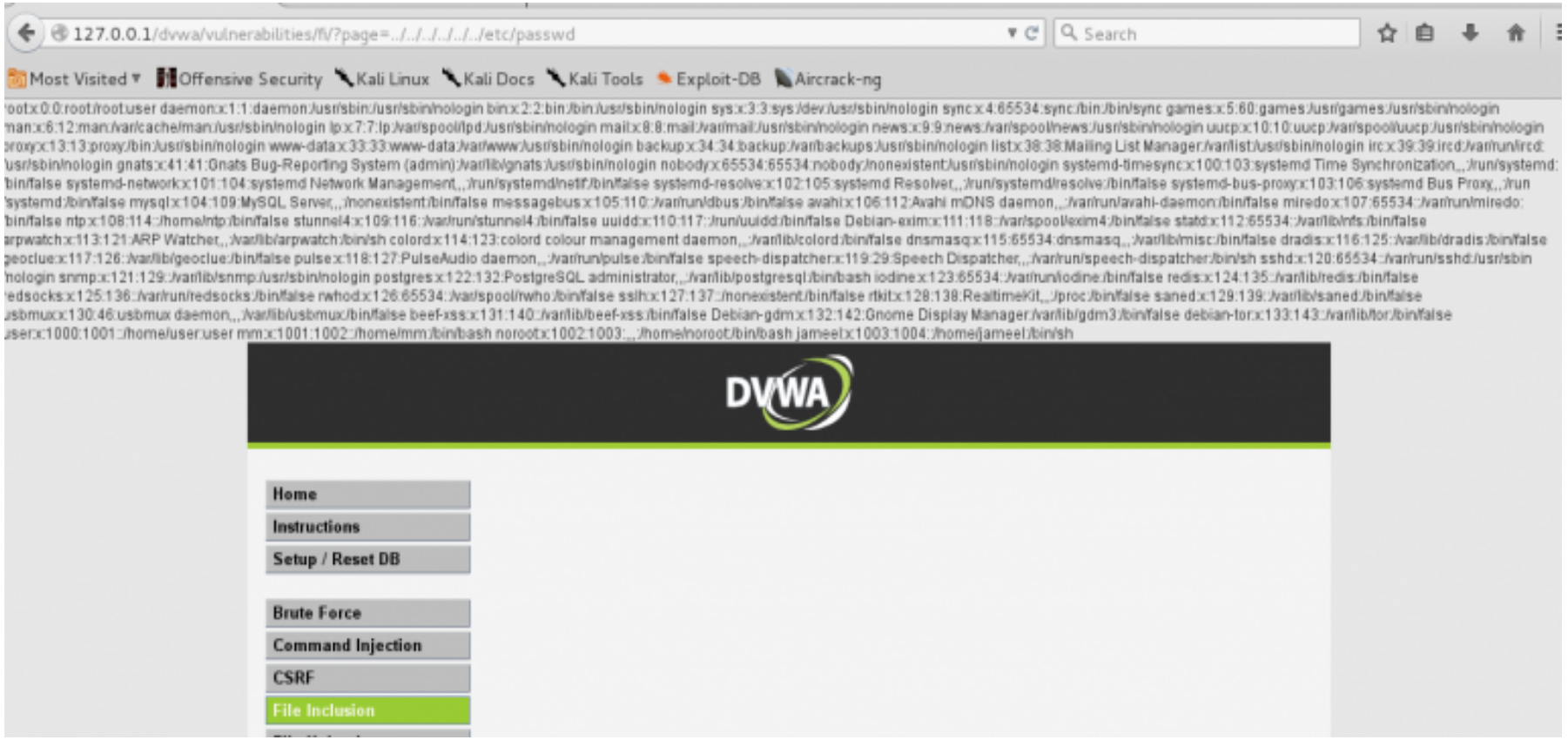
- تنفيذ هجوم تجاوز المسار يسمح لك بالوصول إلى المصادر الغير مصرح لك الوصول إليها.
- فحص هذه الثغرة :
- تعداد عوامل الدخل:
  - من أجل تحديد أجزاء التطبيق المصابة بهذه الثغرة يجب على مختبر الاختراق أن يقوم بتعداد كل الأجزاء التي تقبل دخل من المستخدم وهذا يتضمن طلبات HTTP GET and POST وكذلك كل ال Parameters التي تقبل دخل من المستخدم
- طريقة الفحص:
  - الخطوة التالية هي تحليل طريقة التحقق من الدخل المستخدمة في تطبيق الويب حيث أن مختبر الاختراق يمكن أن يقوم بإدخال " /../../../../etc/passwd " كجزء من عنوان URL من أجل عرض محتوى ملف / etc/passwd والذي يحوي على الهاش hash الخاص بكلمات السر، هذا النوع من الهجمات يمكن أن يحدث عن فشل التحقق من الدخل المقدم من المستخدم.

ثغرة ال Path Traversal (تكمله...)

- لنجاح هذا الهجوم يجب على مختبر الاختراق أن يكون على معرفة بنوع نظام التشغيل الهدف طبعاً لا يمكن طلب الملف / etc/passwd من سيرفر يعمل بنظام (IIS)
- سوف نقوم بهجوم تجاوز المسار (التنقل عبر المجلدات) من أجل الوصول إلى ملفات في سيرفر الويب غير مصرح لنا بالوصول إليها.
- هذه الثغرة تسمح لنا أيضاً برفع ملفات وتغير الإعدادات في سيرفر الويب.
- أول مرحلة في هذا الهجوم هي معرفة المكان الموجودة فيه ملفات تطبيق الويب على السيرفر ومن ثم محاولة الانتقال لمسارات أخرى (مجلدات أعلى) باستخدام التعليمة " /.. " عدد من المرات لاستغلال هذه الثغرة.
- لاختبار هذه الثغرة نستخدم هذه التعليمة " /.. " عدد من المرات إلى أن نحصل على العدد الصحيح وهو عدد المجلدات الموجودة في هذا المسار.

ثغرة ال Path Traversal (تكمله...)

- نتيجة طلب هذا العنوان سوف تعرض محتوى الملف /etc/passwd



ثغرة ال Path Traversal (تكمله...)

- استخدمنا " /.. " 6 مرات من أجل الوصول إلى / etc/passwd وهذا يعني أنه يمكننا الوصول إلى root directory بتجاوز الملفات أربع مرات.

- تمكنا من تجاوز المسار المخصص لتطبيق الويب وقمنا بكشف معلومات حساسة عن السيرفر الهدف.

تم بحمد الله انتهاء الفصل السادس عشر