Path Traversal / Directory Traversal attack

Federico Degan

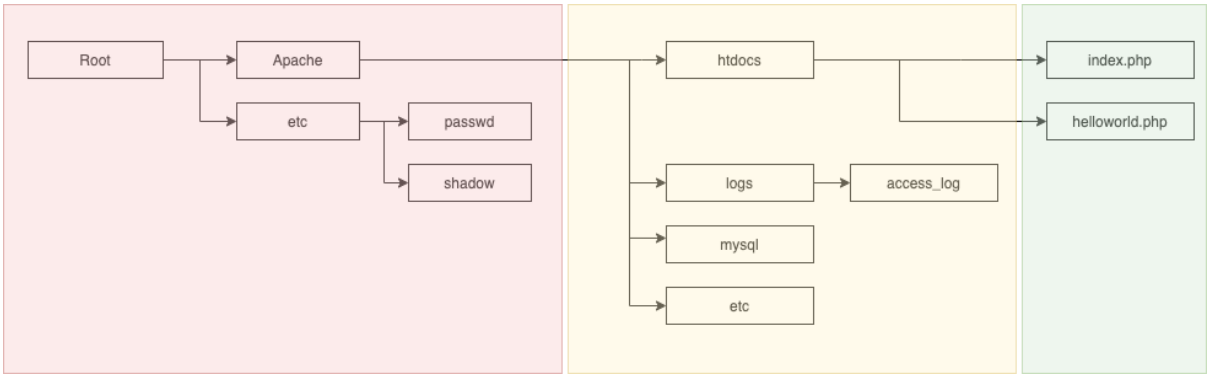
Kurzerklärung und Ausganslage

Bei einer Directory Traversal Attacke oder auch Forceful Brosing genannt verschafft sich der Angreifer Zugang zu Verzeichnissen und Dateien die nicht für diesen gedacht sind.

Die Vorbereitung für einen solchen Angriff sind praktisch nicht existent, da diese einfach durch Pfadangaben in der URL Zeile durchgeführt wird.

Hierbei wird die Standard Verzeichnisstruktur von Webservern bzw. des jeweiligen Betriebssystems ausgenutzt.

Hat man zum Beispiel einen Apache Server auf einer Linux Umgebung so sieht der Pfad zu einem File welches man beim Aufrufen einer Webseite anfordert wie folgt aus:



Hierbei ist der grüne Bereich der Inhalt des Verzeichnisses, auf das der Benutzer Zugriff haben darf, er greift direkt über Links auf diese Inhalte zu, hier können auch beliebige Unterordner mit Bildern für eine Webseite oder weiteren Seiten vorhanden sein.
Es ist angedacht, dass der User sich parallel auf der Ebene bewegt oder weiter nach rechts in Verzeichnisse gehen kann.

Im gelben Bereich befinden sich für den Webserverdienst relevante Verzeichnisse und Dateien.
Hier hat der User keinen direkten Zugriff, es ist jedoch möglich, dass die Applikation ihm Daten zum Beispiel aus einer Datenbank beschränkt zugänglich macht.

Der rote Bereich ist Root Verzeichnis des Servers, hier hat der User keinen Zugriff, da sich hier absolut kritische Daten befinden, die für die Sicherheit des Betriebssystems zentral sind.

Der Angriff

Wenn der Angreifer auf die Webseite zugreift, so sieht er zum Beispiel, dass eine Seite wie folgt aufgerufen wird:

Dies kann ein Hinweis dafür sein, dass der Webserver mittels PHP Funktionen Teilinhalte der Webseite aus anderen Files einliesst.

Hier kommt nun der Exploit ins Spiel:
Man kann in einer URL Zeile wie auf dem Betriebssystem auf welchem der Webserver läuft mittels «/..» auf Linux Systemen oder mit «\..» auf Windows Systemen auf das übergeordnete Verzeichnis springen, wir kennen dies zum Beispiel auch aus dem Terminal mit «cd ..», der Trick dabei ist, dass es keinen Error gibt wenn man zu viele Verzeichnisse hoch springt, man landet einfach immer wieder im Root Verzeichnis.

Gibt es von der Applikation keine Restriktionen diese Zeichen in der URL zu verwenden so kann sich der Angreifer Zugriff auf diverse Dateien und Verzeichnissen im gesamten System verschaffen, wer hier Kenntnisse von der Struktur des Betriebssystems hat kann mit Leichtigkeit an sensible Daten gelangen, wie zum Beispiel dem «passwd» File.
Dieses findet man leicht im root/etc Verzeichnis.
In diesem File findet ein Angreifer zahlreiche vertrauliche Daten über das System wie zum Beispiel alle System Accounts, deren ID, Gruppen IDs, das Home Directory und mehr.
Im etc/shadow File befinden sich sogar die verschlüsselten Passwörter der Benutzer.

Um auf das passwd File zuzugreifen braucht der Angreifer nur eine Linie in der URL Zeile einzugeben:

www.eineDomain.ch/bWAPP/directory_traversal_1.php?page=/../../../../etc/passwd

Der Server springt mehrfach ins Root Directory, geht dann vorwärts ins etc Verzeichnis und liefert der Webapp schlussendlich das passwd File als input, diese stellt diese wie für normale Textfiles auf dem Webserver dann im Browser dar:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

Sicherheitsmechanismen und Fazit

Um dies zu verhindern ist es wichtig, dass die Webapp eine Eingabe von Backtracking Verzeichnislinks nicht akzeptiert, sprich es darf kein «/..» in der URL enthalten sein.

Man könnte auch in der App zuerst den angefragten Verzeichnislink komplett abbilden und feststellen ob sich dieser ausserhalb der Webapplikation befindet und dann blockieren.

Dieser Exploit wird heutzutage von praktisch allen seriösen Frameworks geblockt und er kann nur noch extrem selten angewendet werden, jedoch ist er durch die extrem einfache Anwendung und die mögliche Datenbeute für den Angreifer sehr gefährlich und man muss sich davor auf jeden fall schützen.

Der Angriff benötigt sehr wenige Kenntnisse, keine Vorbereitung, ist in weniger als einer Minute durchgeführt und könnte im schlimmsten Fall das gesamte System und alle darin enthaltenen Daten gefährden.