Fehler in der SQL - Sprache

Beitrag startet hier -> [wiki]Empfindliches PHP - Skript[/wiki]

Der Schlüssel des timing - Angriffes ist es, festzulegen, ob eine Abfrage bezogen auf die Ausführungszeit, erfolgreich war oder nicht.
Mann sollte keine zeitaufwendigen Funktionen, wie „BENCHMARK()“ durchführen. Die lässt sich mit dem Vergleichsoperators „IF()“ beschreiben.So kann man einen SQL – Fehler verursachen, welcher Bedingung abhängig ist.

Ein SQL – Fehler lässt sich erzwingen, indem wenn eine durch „IF()“ geprüfte Bedingung falsch ist. Dazu muss man eine SQL – Nebenabfrage spezifizieren, welche mehr als einen Eintrag zurückschickt.

Daraus Schlussfolgern wir, dass „IF()“ nur für die Eintragungsanzahl einer Tabelle gilt und verursacht, falls die Bedingung falsch ist eine Nebenabfrage (SELECT 0),FROM information_schema.TABLES, diese führt zu dem Resultat, dass mehr als eine Eintragung zurückgesendet wird und daraus ein SQL – Fehler entsteht.Dadurch ist man im Stande, ohne einen timing – Angriff durchzuführen, die von „IF“ ausgehende Bedingung zu prüfen.Dies können wir nun mittels Python testen.

Hier geht es weiter -> [wiki]Abzählung duch COUNT() und LIKE[/wiki]