Empfindliches PHP - Skript

Dieser Eintrag startet hier [wiki]Blinde SQL - Injektion - Gefahren und Maßnahmen[/wiki] == Das Zielskript ==

Quellcode

```
1. <?php
2. mysql_connect('location','test','test');
3. mysql_select_db('test')
4. $id = $_GET['id'];
5. if ($id!='')
6. $query ="SELECT id,name FROM products WHERE id=" .$id." LIMIT 1"
7. $res = mysql_query($query);
8. if ($res!=NULL) { echo('Coto voir article'); mysql_free_result ($res)}
9. }} else {
10. ?>
11. <html>
12. <head> <title>SQL Injection: demo</title> </head>
13. <body>
14. <form action='' methode'GET'>
15. ID Article:<input type="text" name="id"><br>
16. <input type="submit" value="View"
17. </form>
18. </body>
19. </html>
20. <?php
21. }
22. ?>
```

Alles anzeigen

Zuerst müssen wir vermerken, dass die Variable „$id“ als ganze Zahl betrachtet wird, denn sie darf nicht durch das Skript gefiltert werden. Man kann annehmen, das die Zeichenkette in der Abfrage, später mit Hilfe des Operators von MySQL mir CHAR() kodiert wird. Wenn die Zahl in der Eintragung in der Tabelle information _schema.TABLES kleiner als 1 ist, dann braucht die Abfrage eine bestimmte Zeit, um ausgeführt zu werden, dies spiegelt sich dann auf die Ladezeit der HTML – Seite wieder. Nach einer gewissen Anzahl an Injektionen, ist man nun im Stande, die genaue Anzahl an Tabellen, die für den Benutzer zugänglich sind, zu bestimmen. Diesen Vorgang, kann man auch anwenden um die Zahl von Benutzern auf einer Internetseite festzulegen. Beim beschriebenen timing – Angriff, gibt es jedoch mehrere Schwachstellen.

- Der Befehl „IF()“ gilt nur für alle zurückgelieferten Eintragungen, dessen Zahl muss auf 1 gesetzt erden. Mit „COUNT()“ kann diese umgangen werden.
- Man braucht viel Zeit um die Gesamtheit der Dateien, wieder zu gewinnen

Es muss also ein wirkungsvollerer Angriff gefunden werden, der nach einen Prinzip vorgeht, indem Ladezeiten nicht mit untergebracht sind. Hört sich im ersten Moment komisch an, doch dies geht. Weiter geht es hier -> Dieser Eintrag startet hier [wiki]Fehler in der SQL - Sprache[/wiki]