4 אפריל 2018
י"ט ניסן תשע"ח
סימוכין: ב-ס-572

Web Shell – יכולות, מניעה וזיהוי

תקציר

Web Shell הינו סקריפט (SCRIPT) המותקן על ידי תוקף על גבי שרת WEB. השרת יכול להיות נגיש ברשת האינטרנט (המקרה הנפוץ) או שרת פנימי ברשת הארגונית.

הסקריפט מאפשר לתוקף גישה אל השרת וביצוע פעולות שונות עליו, בהרשאות של שרת ה- WEB, כמו גם דרך יעילה להרחבת הנגישות אל תוך הרשת הארגונית, וצינור יעיל להוצאת מידע ממנה החוצה (כאשר השרת נגיש לרשת האינטרנט).

מסמך זה יתאר מהו Web Shell ויכולותיו, כיצד ניתן להתגונן מפניו, וכיצד לזהותו.

פרטים

יכולות ה- Web Shell

Web Shell יהיה כתוב בשפת סקריפט הניתנת להפעלה על גבי שרת ה- WEB המותקף. בדרך כלל מדובר על ASP או PHP, אך נצפה שימוש גם בשפות נוספות כגון PYTHON, PERL, RUBY וכדי.

הסקריפט מאפשר גישה לשרת והפעלה של משאביו השונים, והוא יכול להיות פשוט או מורכב מאד כרצון התוקף. ישנם Web Shell מתוחכמים המהווים למעשה ממשק ניהול מלא **שאינו מורשה** על השרת, וישנם כאלו המורכבים משורה בודדת, אשר מעבירה את הפקודה שרושם התוקף, לביצוע על ידי מערכת ההפעלה של השרת המותקף.

לדוגמה, הסקריפט הבא מעביר לביצוע על ידי מערכת ההפעלה את הפקודה שכותב התוקף:

```
<?php
  echo(system($_GET["q"]));
?>
```

הפעלת פקודה כגון ls תיראה כך:

http://example.com/Web Shell.php?q=ls

הפלט יהיה רשימת הקבצים והספריות תחת הספריה הנוכחית בשרת המותקף.

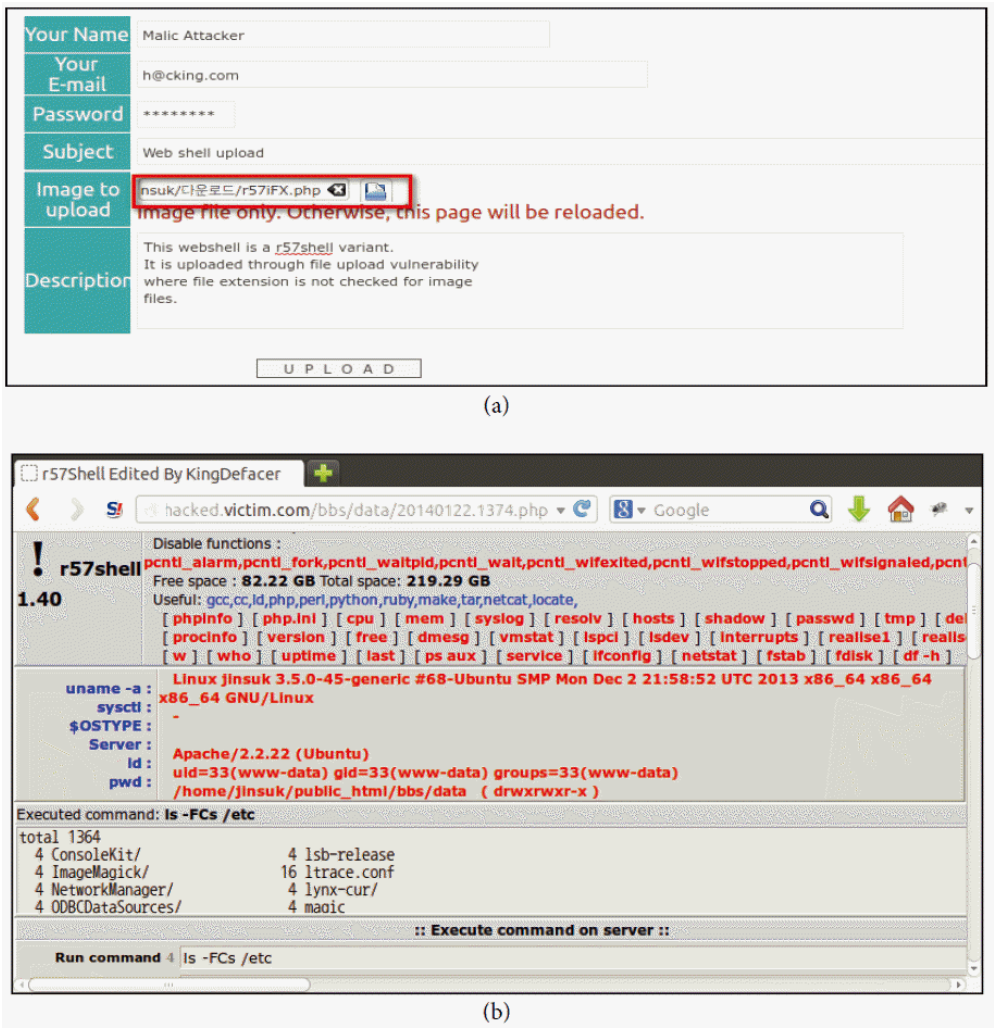
דוגמה נוספת:

```
<pre><body bgcolor=white><? @system($_REQUEST[“cmd”]); ?></body></pre>
```

מאפשר לתוקף הרצת פקודות כך:

http://www.victom.com/upload/simple-cmd.php?cmd=cat+/etc/passwd

הפלט יהיה קובץ הסיסמאות של השרת.

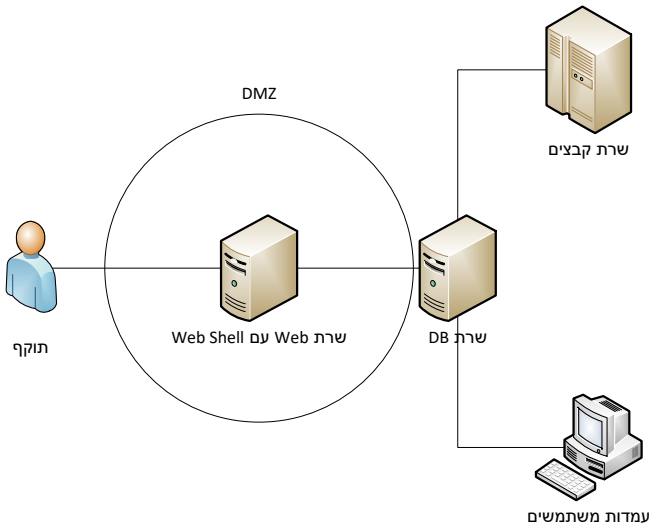


צילום מסך של r57shell version 1.40[1]

מעבר ליכולות התקיפה על שרת ה- WEB עצמו, ישנם שרתי WEB המקושרים למערכות ארגוניות נוספות, כגון שרתי בסיסי נתונים, כך שה- Web Shell מעניק לתוקף וקטור תקיפה התחלתי כנגד מערכות אלו.

לדוגמה, באיור הבא אנו רואים כי תוקף אשר השיג אחיזה בשרת ה- WEB והתקין עליו Web Shell, יכול לנצלו לתקיפת שרת ה- DB המשרת את האתר, וממנו להתפשט לעמדות ושרתים נוספים ברשת הארגונית.

[1] https://doi.org/10.3745/JIPS.03.0026



שרטוט המתאר את התקיפה

בניגוד לכלי תקיפה היוזמים תעבורה אל כתובות מסוימות ברשת, ובכך מקלים לעיתים על זיהוים, Web Shell הינו סקריפט הפועל על שרת אשר מעצם ייעודו מקבל כל הזמן פניות מהרשת, עובדה זו מוסיפה קושי לזיהוי.

דרכי התמודדות

1. מניעה

להלן המלצות לפעולות למניעת התקנתו של Web Shell על שרת ה-WEB:

1.1 הקשחה

על מנת להעלות Web Shell לאתר, התוקף צריך לנצל פגיעות קיימת. לרוב פגיעויות אלו יהיו קשורות להגדרות לא מאובטחות של השרת או לשגיאות תכנות.
נדרשת הגדרה נכונה של שרת ה- WEB, בהתאם ל- Best Practices מוכרים ועל פי העיקרון של Least Privilege.
אם השרת מאפשר העלאת תוכן על ידי המשתמשים, כתיבת התוכן, לאחר בדיקתו, רק לספריה ייעודית לכך.
שמירה על עקרונות התכנות המאובטח של השרת, ומניעת תקיפות המאפשרות העלאת קבצים בלתי מורשית על ידי התוקף. במיוחד יש להימנע מפגיעויות מן הסוגים הבאים:

- Cross-Site Scripting
- SQL Injection
- Remote File Include (RFI) and Local File Include (LFI)
- ממשקי ניהול חשופים לרשת האינטרנט

1.2 התקנת עדכוני אבטחה

יש לעקוב באופן עיתי אחר אתרי היצרנים ולהתקין בהקדם האפשרי, ולאחר בדיקה, כל עדכון אבטחה שהיצרנים מוציאים עבור שרת ה- WEB ומערכת ההפעלה עליה הוא פועל.

1.3 סגמנטציה ובקרת תעבורה

אין לאפשר לשרת ה- WEB גישה חופשית למשאבים רשתיים. יש לנטר תעבורת הרשת אל השרת וממנו, ולאפשר גישה אליו רק בפרוטוקולים ובפורטים הרלוונטיים (בדרך כלל פורטים 80 ו- 443, תעבורת HTTP/S). תעבורה יוצאת מן השרת תאופשר אך ורק אל שרתים שיש לו צורך בגישה אליהם, כגון שרת DB, ובפורט המתאים בלבד.
שרת ה- DB שבשימוש שרת ה- WEB לא ימוקם בתוך הרשת הארגונית אלא ב- DMZ ייעודי, וגם אליו וממנו תהיה בקרת תעבורה קפדנית לסיכול ניצולו כווקטור תקיפה כלפי הרשת הארגונית.

1.4 שימוש ב- WAF (Web Application Firewall)

WAF הינו ציוד או שירות ייעודי לניטור ובקרה על תעבורה לשרתי WEB. מומלץ לעשות שימוש ב- WAF על מנת לסכל ככל האפשר את התקיפה הראשונית המאפשרת התקנת Web Shell, וכן פניה של התוקף להפעלת ה- Web Shell.

2. <u>זיהוי</u>

להלן המלצות לזיהוי Web Shell אשר הותקן על השרת:

2.1 ניטור

- יש לנטר אירועים חריגים בשרת, כגון הפעלה של Command Line (CMD/BASH) או פקודות אחרות שאינן מתוכננות לשימוש בשרת.
- ניטור של אחוז שימוש גבוה ב- CPU כאשר התעבורה לאתר אינה גבוהה.
- ניטור שינוי בקבצים בשרת, הוספה של קבצים חדשים או שינוי בקבצים קיימים שלא על ידי מנהלן מוסמך של הארגון. השוואה כזו ניתן לבצע באמצעות שמירת HASH קריפטוגרפי של הקבצים המותקנים בשרת, והשוואתם כנגד HASH של הקבצים הקיימים בפועל בספריות הקוד של השרת. יש לעדכן את ה- HASH לאחר כל שינוי או עדכון יזום של הקוד בשרת. לחילופין ניתן לשמור SNAPSHOT של הספריות והקבצים בשרת, ולהשוות מול הקבצים המותקנים בפועל.
- לזיהוי השינויים הללו ניתן להיעזר גם במערכות מסוג File Integrity Monitoring – FIM. אם מערכת ניהול התוכן של האתר תומכת בזיהוי שינויים כאלו, ניתן להיעזר בה.
- זיהוי קבצים בעלי חתימת זמן מאוחרת יותר ממועד העדכון האחרון של השרת.

2.2 לוגים

יש לנטר את קבצי הלוג של השרת לזיהוי פניות חריגות אליו וממנו. לדוגמה:

- פניות והזדהות משרתים ותחנות ברשת הארגונית אל שרת ה- WEB, שלא בהתאם לאפיון המקורי של האתר
- שימוש בפקודות למעבר ספריות (Directory Traversal)
- גישה ישירה אך ורק ל- URL מסוים
- ניתוח סטטיסטי של פניות ל- URL (בדרך כלל יהיו מגוון של USER AGENTS בפניות. ל- WEB SHELL אמור לגשת רק התוקף, לכן צפוי שימוש ב- USER AGENTS בודדים או ייחודיים).
- פניות חוזרות ל- URL מסוים ללא שדה REFERER עלול להצביע על שימוש ב- Web Shell.

2.3 הפעלת כלי חיפוש ייעודיים

קיימים כלים ייעודיים המאפשרים חיפוש אחר Web Shell בשרת. אחד מהם הוא הכלי Web Shell Detector. את הכלי מתקינים כסקריפט על השרת ומפעילים אותו באמצעות הדפדפן, או משורת הפקודה. הכלי כולל חתימות לזיהוי של מעל 600 Web Shell שונים. היצרן מפעיל גם שירות חינמי המאפשר להעלות אליו קבצים החשודים כ- Web Shells, לצורך ניתוח.
תשומת לב כי כלים אלו עלולים לעיתים לתת זיהויים שגויים (False Positives).

2.4 שימוש ב- AV

במידה שמותקן על השרת מנוע AV, עשוי גם הוא לסייע בזיהוי של Web Shell, אם כי אחוזי הזיהוי אינם גבוהים בדרך כלל.

2.5 YARA

קיימים מאגרים של חוקי YARA המיועדים לזיהוי Web Shell. ניתן להריץ חיפוש YARA על ספריות השרתים באמצעות חתימות אלו.

3. הסרה והתאוששות

במידה ונמצא בארגונכם Web Shell, מעבר להתקנה מחדש של השרת והאתר ממדיה בדוקה, ושינוי כל סיסמאות הגישה אליו, יש לוודא שינוי כל סיסמאות הגישה גם אל השרתים שהוא נגיש אליהם כגון שרתי DB.
במידה שבבדיקתכם התגלה ממצא כלשהו נבקש לקבל היזון חוזר. לכל מידע נוסף ניתן לפנות אלינו.

הערה: שיתוף מידע עם ה- CERT הלאומי איננו מחליף חובת דיווח לגוף מנחה כל שהוא, במידה שהתגלה צורך כזה.

בברכה,
CERT-IL
טל: 9344*
team@cert.gov.il