Digital Whisper
Technologic Papers

טיפים לשיפור אבטחת WordPress

מאת שחר גלעד

הקדמה

WordPress החלה את דרכה כפלטפורמה לכתיבת בלוגים במתכונת של קוד פתוח. מה שאומר שכל אחד יכול לעצב אותה כראות עיניו, לכתוב שורות קוד נוספות ולבנות עבורה תוספים ייעודיים. עם הזמן הפלטפורמה התפתחה מבניית בלוגים קטנים וחביבים, לאחת מהפלטפורמות המובילות ביותר בעולם לבניית אתרים! בזכות הקוד הפתוח והעובדה שכל מפתח יכול להוסיף ולשפר אותה, גדלה WordPress לממדים עצומים, וכיום 25 אחוז מכלל האתרים באינטרנט בנויים על WordPress.

הפופולאריות העצומה שלה והעובדה שהיא קלה ונוחה לתפעול, מאפשרת לאנשים רבים, שלא כתבו שורת קוד אחת ומעולם לא עסקו בתכנות, לבנות אתרים יפים שבהחלט מסוגלים לספק לא מעט מהצרכים הקיימים היום. בזכות הקלות והממשק הנוח לתפעול, חברות רבות בונות ללקוחות אתרים ב-WordPress ולאחר הדרכה קצרה בעל האתר יכול לנהל את התכנים שלו באופן עצמאי. שימוש ב-WordPress מקטין בצורה ניכרת את התלות של הלקוח בחברה שבנתה לו את האתר, דבר שלעתים רבות משרת הן את אינטרס הלקוח והן את אינטרס החברה.

אז איך למעשה הפלטפורמה עובדת?

אחד היתרונות הגדולים במערכת, היא האפשרות לרכוש תבניות מוכנות מראש. כלומר, מתכנתים יושבים ויוצרים תבנית בדיוק כמו שהאתר נראה לכל עניין ודבר. את התבנית רוכשים, מתקינים על WordPress ובעזרת הממשק הנוח לתפעול, כל שנותר לעשות הוא להוסיף תכנים, תמונות, לשנות צבעים, לתת קצת טאץ' אישי והנה לכם אתר מוכן.

ל-WordPress יש אלפי תוספים, גם חינמיים וגם בתשלום, שבעזרתם ניתן לייעל את האתר עוד יותר. מחפשים אפשרות קצרה לחבר בין האתר לעמוד הפייסבוק העסקי ולא רוצים להתעסק עם קוד? שום בעיה. תוסף ייעודי יעשה את העבודה. זקוקים להטמעה של טפסי "צור קשר" מעוצבים? גם את זה ניתן להתקין בנפרד. למעשה, כמעט כל פיצ'ר שהייתם רוצים לראות באתר שלכם, ניתן למצוא כתוסף (Plugin), להתקין אותו בלחיצת כפתור וליהנות מהעולם הנפלא הזה שנקרא קוד פתוח. לא עוד מערכות סגורות שרק מתכנת אחד או שניים, אשר עבדו על האתר יוכלו לשנות, אלא מערכת פתוחה הניתנת לשינויים בכל רגע נתון. כמובן שהתוספים החשובים ביותר שיש להתקין לכל אתר הם דווקא התוספים שלא רואים על האתר עצמו. מדובר בתוספי אבטחה חשובים מאוד, כאלו שימנעו מכל מיני אנשים לא רצויים להשתלט לכם על האתר - ועל חלקם אף נרחיב בהמשך.

WordPress, מעצם היותו קוד פתוח, מהווה מטרה נוחה יותר להאקרים שמחפשים לפגוע בכם ובעסק שלכם. ישנה תחרות קבועה בין האנשים שמנסים לפרוץ לאתרי WordPress, למתכנתים שאחראים על תוספי האבטחה. האקרים מנסים להקדים את המתכנתים ולהפך. לזכותם של תוספי האבטחה אפשר לשייך את העובדה, שכאשר מתקינים תוסף, לא מדובר בפעולת שגר ושכח. כלומר, לא התקנתם תוסף אבטחה וזהו, עכשיו 10 שנים הוא יוכל להגן עליכם, וזאת מכיוון שהוא לא יהיה רלוונטי לכלים החדשים של האקרים. תוספי האבטחה ב-WordPress מתעדכנים על בסיס קבוע, מה שמאפשר שקט נפשי, וגם עם האקרים מצאו שיטות עקיפה חדשות, תוספי האבטחה הרלוונטים יעודכנו בהתאם ויסגרו חורים לא רצויים שניתן למצוא בין שורות הקוד. WordPress מעצם היותה קהילה גדולה, ניזונה גם מדיווחים של בוני אתרים אחרים שמאתרים פריצות אפשריות. אותם דיווחים עוברים לאנשים הרלוונטיים, כמו מפתחי תוספים או לאתר WordPress עצמו, והם מצידם מנסים לייעל את המערכת על פי דיווחים אלו.

אבטחה ב-WordPress

בעולם מושלם היה ניתן להמנע ב-100% מפריצות לאתר הנמצא בבעלותינו. אבל אנחנו חיים בעולם בו תמיד יהיו כאלו שינסו להשתלט לכם על האתר, כל פורץ וסיבותיו הוא: זה יכול להיות למטרת שעשוע, מטרת כופר (ידרשו ממכם לשלם כסף בשביל לקבל את האתר בחזרה), או אפילו בגלל איבה פוליטית (ובישראל אתרים תמיד נמצאים על הכוונת של ארגונים פרו-פלסטינים). האבטחה ב-WordPress לא תמנע 100 אחוז פריצות, אבל בעזרת הפעולות הנכונות והתופסים הנכונים היא בהחלט יכולה לצמצם בצורה משמעותית את אפשרויות הפריצה לאתר שלכם.

איך עושים את זה בפועל?

עוד לפני שניגע בתוספים, קיימים מספר שלבים אותם צריך לבצע על מנת לאבטח את ה-WordPress שלכם. יש לבצע חלק מהצעדים עוד בשלב הקמת האתר ואת השאר מבצעים בצורה שוטפת:

Antivirus למחשב - במידה והמחשב שלכם נגוע בווירוסים שאוספים עליכם מידע, יהיה קל מאוד לאותו האקר לגנוב לכם את סיסמאות הניהול ולהשתלט לכם על האתר. על כן יש להקפיד כי המחשב שלכם נקי מתוכנות מסוכנות ולהתקין Antivirus, שמתעדכן וסורק את המחשב שלכם על בסיס קבוע כי אם במקרה יש לכם תולעים או סוסים טרויאנים הם דיי בקלות יכלו לזהות את השם משתמש וסיסמא למערכת ניהול של האתר שלכם.

Hosting - בראש ובראשונה, אל תתפתו לאחסן את האתר שלכם על שרת רק כי הוא זול. תעשו בדיקה מקיפה. תקראו המלצות וחוות דעת על חברות האחסון השונות ותוודאו כי השרת עליו אתם מאחסנים את האתר, תמיד לבדוק שהחברת אחסון שאצלם אתם מאחסנים מבצעים גיבוי לאתר יום יום וכמובן לבדוק

האם הם משתמשים בשרתים שלהם בשפת קוד PHP (השפת קוד של WordPress) הכי חדשה בשוק, כי אם לא הפרצות יכולות להגיע גם דרך השרת אחסון.

הגנה על ממשק הניהול - למרות שזה נשמע טריוויאלי, מדובר בצעד סופר חשוב שיש להקפיד לעשות. ברגע שה-WordPress הותקן על הדומיין, בונה האתר מתבקש לבחור שם וסיסמא. כמו בפייסבוק שלכם או בג'ימייל, חשוב מאוד שהסיסמא לא תהיה פשוטה, כמו לדוגמה הספרות 1-8. אלא סיסמא מסובכת שתערב תווים מיוחדים, אותיות גדולות ומספרים (אמנם זה לא חובה אבל זה בהחלט מומלץ) כמובן, שגם את שם המשתמש שלכם לא כדאי להשאיר כ-Admin, שזה מה שתקבלו כברירת מחדל, אלא לשנות לשם קצת יותר מורכב. את הפעולה הזאת מבצעים פעם אחת כשמקימים את האתר, וכמובן שניתן לשנות סיסמא בכל רגע נתון, לא מעט פעמים נתקלתי באתרי לקוחות שהשם משתמש הוא Admin והסיסמא היא 12345 אז חשוב לדאוג לזה כי אלו הסיסמאות הכי קלות לפרצה על ידי האקרים. החוק החשוב ביותר בעת בחירת סיסמה הוא: "סיסמה שקל לזכור אך קשה לנחש".

עדכוני גירסה שוטפים - WordPress, כאמור, היא פלטפורמה שכל הזמן מתעדכנת, כל הזמן מנסים לשפר אותה ולייעל אותה, ולכן היא זוכה לעדכוני גירסה על בסיס קבוע. אחת לכמה זמן, יוצא לאוויר העולם עדכון גירסה, שבין היתר מתייחס לפריצות אפשריות וכמובן שהוא נועד גם לחסום אותם. את עדכון הגירסה אפשר תמיד לבצע דרך האתר של WordPress. אפשר להגדיר במערכת הניהול שלכם, שההגדרות יבוצעו אצלכם בצורה אוטומטית וכל פעם שיהיה עדכון, המערכת שלכם תעודכן. חברת אחסון אחראית שולחת התראה ללקוחות שמאחסנים אצלה אתר על כך שקיים עדכון וניתן לבצע אותו, לכן בעל אתר לא יוכל להגיד "לא ידעתי", וכאשר יש עדכון, חשוב מאוד לבצע אותו.

אותה הפעולה חלה גם על תוספים. הפלאגינים המותקנים על האתר, גם הם זוכים לטיפול מקיף ובתדירות די גבוהה ניתן למצוא להם עדכונים. חשוב להקפיד לעדכן אותם. זכרו, כל גירסת WordPress או תוספים לא מעודכנת, עלולה להיות הדלת שדרכה האקרים יפרצו לאתר שלכם. הקפידו לעדכן!

FTP - אם אתם מעלים את התבנית, קבצים ושאר התיקיות של האתר שלכם דרך FTP, תנסו לעבוד דרך ממשק ה-SFTP. שימוש בו זהה לחלוטין ל-FTP. ההבדל היחיד הוא שב-SFTP, כל הסיסמאות ותווך התקשורת שלכם מוצפן ואינו עובר לשום מקום לא צפוי. ככה שגם אם במהלך תהליך העברת הקבצים מ-FTP לשרת מחכה לכם פורץ, הוא לא נחשף לסיסמאות שלכם.

שמירה על ה-Database - במידה ואתם מאחסנים מספר אתרים על אותו השרת מומלץ להקפיד להקים עבור כל אחד משתמש בנפרד.

אבטחת קובץ WP-CONFIG.PHP - ניתן להעביר את הקובץ לתיקיה שנמצאת מעל ההתקנה של ה-WordPress. כלומר האתר יושב בתיקיית ה-root, אך הקובץ של WP-CONFIG.PHP נמצא בתיקיה אחרת כך שלא יהיה ניתן לגשת לקובץ הנ"ל ללא גישה למערכת הקבצים של השרת.

ניטרול עריכת קובצים - לפי הגדרות ברירת המחדל של WordPress, כל אחד יכול לערוך את קבצי ה-PHP לפי הצורך. שינויים כאלו ואחרים אמנם יכולים לסייע לכם בהטמעת קוד, אך לרוב הם גם יהיו המקום הראשון שאליו תוקפים ינסו להגיע בשביל לחרב לכם את הקוד ולשתול שם את הדברים שלהם, אם פרצו לאתר שלכם ודרך הממשק ניהול יש אפשרות לערוך קבצים הפורץ יכול בקלות לשנות ולמחוק את כל האתר בלי בעיה. לכן הקפידו לחסום עריכת קבצים דרך הממשק ניהול.

גיבויים על בסיס שוטף - וודאו כי חברת האחסון עליה יושב האתר שלכם מגבה את התכנים והגירסאות האחרונות של האתר. אם יש משהו יותר נורא מפריצה לאתר, זה היום שאחרי, שהפריצה נסתמת וההאקר נעלם ואין לכם גיבוי. במצב כזה תצטרכו להתחיל לבנות את כל האתר ולהזין את כל התכנים מאפס. מן הסתם, אף אחד לא מעוניין בעבודה שכזו, לכן חשוב לוודא כי יש לכם קבצי גיבוי שמתעדכנים כל הזמן, לכל צרה שלא תבוא.

תוספים (פלאגינים) לWordPress

כאמור, מעבר לשיטות האבטחה שניתן לעשות "בידיים", קיימים תוספי אבטחה ייעודיים ל-WordPress. עדיין לא נוצר התוסף האחר שמצליח לכסות על הכל ויכול להעניק הגנה של 100%, אך אפשר להשתמש בשילוב של תוספים על מנת לאבטח את האתר בצורה המקסימלית. חשוב לדעת כי תוספים מצויינים מסויימים, יכולים להגן על רבדים שונים באתר, אבל לא על הכל בבת אחת. עובדה חשובה נוספת לגבי תוספים - אם ניסיתם תוסף למען מטרה מסויימת והחלטתם לא להשתמש בו, תמחקו אותו. אל תשאירו אותו במצב לא פעיל, אלא פשוט תמחקו אותו מהמערכת שלכם. תוסף לא פעיל שיושב אצלכם על האתר, הוא לא תוסף שאתם מעניקים לו תשומת לב. **הזמן יעבור, לא תעדכנו אותו והוא יוכל להפוך לפתח עבור פורצים**. אם אתם לא זקוקים לתוסף, הסירו אותו מהאתר ומהשרת שלכם. **תישארו רק עם התוספים החיוניים לכם**, והקפידו לוודא כי הם מתעדכנים על בסיס קבוע.

All in One WP Security & Firewall plugin - תוסף פופולארי במיוחד, עם מספר פונקציות חשובות במיוחד.

אבטחת חשבונות משתמשים:

- התוסף מזהה חשבונות משתמשים בשם "Admin" ומתריע לך לשנות אותם, בנוסף הוא מזהה אם השם משתמש והסיסמא זהים (אני לא צריך לפרט כמה שזה אידיוטי, אך יש לא מעט אתרים עם כאלו פרטי גישה)
- הפלאגין כולל כלי שיוצר לך סיסמא חזקה ביותר הרבה מאשר הסיסמאות ש-WordPress מיצר.

אבטחת כניסת משתמשים למערכת ניהול:

- על מנת למנוע התקפה באמצעות כניסות מרובות, התוסף חוסם את ה-IP מחוץ למערכת ומתריע לך על זה במייל, התוסף גם מאפשר לך לחסום או לבטל חסימה לכתובות IP מרובות בלחיצת כפתור.
- מנתק משתמשים לאחר שהייה רבה מדי במערכת ללא כל פעולה (על מנת לבלום תקיפות)
- הפלאגין כולל אפשרות לראות את רשימת משתמשים אשר מחוברים בזמן אמת לאתר שלך.
- הפלאגין כולל אפשרות להוסיף קאפצ'ה בכניסה למערכת ניהול "ולשכחתי סיסמא" על מנת למנוע מסקריפטים אוטומטיים לבצע Brute Force לממשקי הניהול.

אבטחת מסד נתונים:

- בלחיצת כפתור תוכל ליצור גיבוי למסד נתונים בכל זמן שתרצה.

אבטחת מערך הקבצים:

- מזהה איזה קבצים או תיקיות ישנם הגדרות הרשאה לא מאובטחות ומתריע לך עליהם על מנת שתסגור את אפשרות הזו.
- מונע שינוי או ערכית קבצי PHP מאזור מערכת ניהול WordPress.

גיבוי ושחזור htaccess ו-wp-config:

אולי החלק הכי חשוב בתוסף, קובץ htaccess מאשרלשלוט בכמעט כל אספקט ברמת השרת, הרבה גורמים זדוניים מנסים לגשת לקובץ htaccess ולערוך אותו, לכן חשוב במיוחד לגבות ולדאוג לשים את הקובץ במקום מוגן. הגיבוי ישמש אתכם למקרה שתרצו לשחזר פונקציות חשובות באתר.

אפשרות לרשימה שחורה:

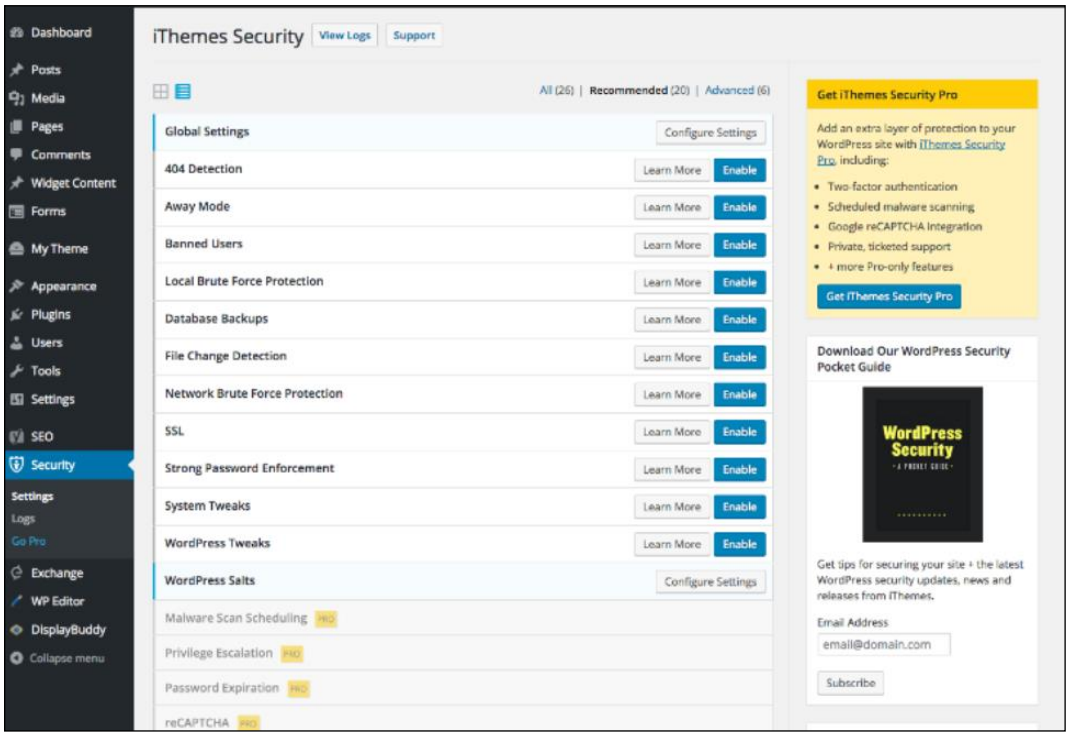
- בליחצת כפתור תוכלו ליצור רשימת IP שאותם תרצו לחסום מהאתר לגמרה.

סריקת אבטחה למסד נתונים ולקבציי האתר:

- סריקה אשר מזהה אם חל שינוי בקבצי נתונים באתר, מראה לך בצורה פשוטה איזה שינויים בוצעו כך שתוכל לדעת אם הם תקינים ואם הכניסו קוד שלא היה אמור להיות קיים שם בכלל.
- סריקה מעמיקה יותר של מסד הנתונים יאפשר לכם לראות אם בוצע שינוי בקבצי JavaScript ו-HTML בליבת המערכת WordPress.

תוסף אבטחה רציני מאוד עם עוד המון פונקציות שתוכלו לקרוא עליהם בעמוד התוסף.

iThemes security - גם הוא תוסף פופולארי, שמתאים גם למשתמשים חדשים וגם למשתמשים מנוסים.



לחיצה אחת תתקין את התוסף לפי הגדרות ברירת המחדל של המערכת (שאמורות לעשות את העבודה), ולמשתמשים בעלי ניסיון רב יותר יש אפשרות להגדיר ולשנות דברים לפי הצורך שלהם. חלק מהתכונות המעולות של התוסף הזה:

הפיצ'ר הכי משתלם - הגנה נגד מתקפות Brute Force עתידיות:

התוסף מזהה ניסיונות פריצה לאתרים אחרים (אשר מותקן בהם התוסף) ואוטומטית חוסם את כתובת ה-IP גם באתר שלך.

פיצ'רי הגנה נוספים:

- התוסף מזהה וחוסם רובוטים אשר מנסים להיכנס למכרת ניהול.
- התוסף מכריח את המשתמשים לשנות את הסיסמא למערכת ניהול לסיסמה שתעמוד במדיניות של סיסמה חזקה, ובנוסף גם מתריע כל פרק זמן להחליף סיסמא.
- התוסף מכבה את אפשרות עריכת הקבצים דרך הממשק משתמש (קבצי PHP ו-CSS שונים), כך שאם בכל זאת מתבצעת פרצה כל קבצי האתר מוגנים.
- התוסף מזהה וחוסם התקפות של רובוטים על המסד נתונים של האתר.

פיצ'רי זיהוי והתרעה:

- התוסף מזהה אם בוצעו שינויים בקוד של האתר ומודיע לך עליהם, כך שאף אחד לא יוכל לבצע שינויים מפגעים מבלי שתקבל התרעה על כך.
- מזהה שינויים קריטיים שבוצעו בקוד וחוסם את האפשרות הזאת.
- התוסף מריץ סריקות, מזהה ומתריע אם באתר שלך זוהה תוכנה זדונית.
- התוסף שולח מייל לבעלים של האתר על כל ניסיון כניסה דרך המערכת ניהול שנכשל.

תוספות נוספות:

- ישנה אפשרות באמצעות התוסף לשנות את ה-URL הקבוע של הכניסה למערכת ניהול (wp_admin).
- מבצע ניתוק אוטומטית מהמערכת ניהול כאשר המשתמש נשאר מחובר אך לא ביצע שום פעולה זמן רב.
- מזהה דפי 404 באתר ומתריע לך על התיקון שלהם לצורכי SEO.

Wordfence Security - תוסף שהותקן למעלה ממיליון פעם, הוא מספק הגנה מפני תולעים וסוסים טרויאנים. התוסף הוא חינמי לגמרה וגם מגיע בקוד פתוח. אך ישנה אפשרות לגירסה בתשלום שמעניקה לך תמיכה מתמדת, חסימה לפי ארצות, בדיקת IP של האתר אם הוא הוספם ועוד...

אך בגדול הגירסה החינמית הינה מספיקה ומציעה מגוון רחב של פיצ'רים:

Firewall:

- התוסף מזהה וחוסם ניסיונות פריצה ממקורות זדוניים ידועים וחוסם את המקורות האלו עוד לפני שניסו לפרוץ לאתר שלך.
- התוסף חוסם איומים שונים כגון: חיקויים של הבוטים של גוגל ורשתות האקרים ידועות.

חסימות באמצעות התוסף:

- כמו התוספים הקודמים, גם כאן ישנה אפשרות לחסום IP לפי בחירתנו.
- התוסף מזהה ניסיונות תקיפה שבוצעו באתרים אחרים ברשת עם אותו תוסף וחוסם אצלך באתר את כתובת ה-IP של התוקף.

- משתמשים בגירסה בתשלום יכולים לחסום כתובת IP אשר מגיעות ממדינות שונות שהם רוצים לחסום.

אבטחת כניסה למערכת:

- התוסף מאפשר לך ביצוע דו שלבי של כניסה למערכת ניהול, תהליך ראשוני יהיה באמצעות סיסמא והתהליך השני באמצעות שליחת הודעה לסלולר שלך.
- התוסף כמו הקודמים לו מכריח אותך לייצר סיסמא קשה.

סריקות אבטחה:

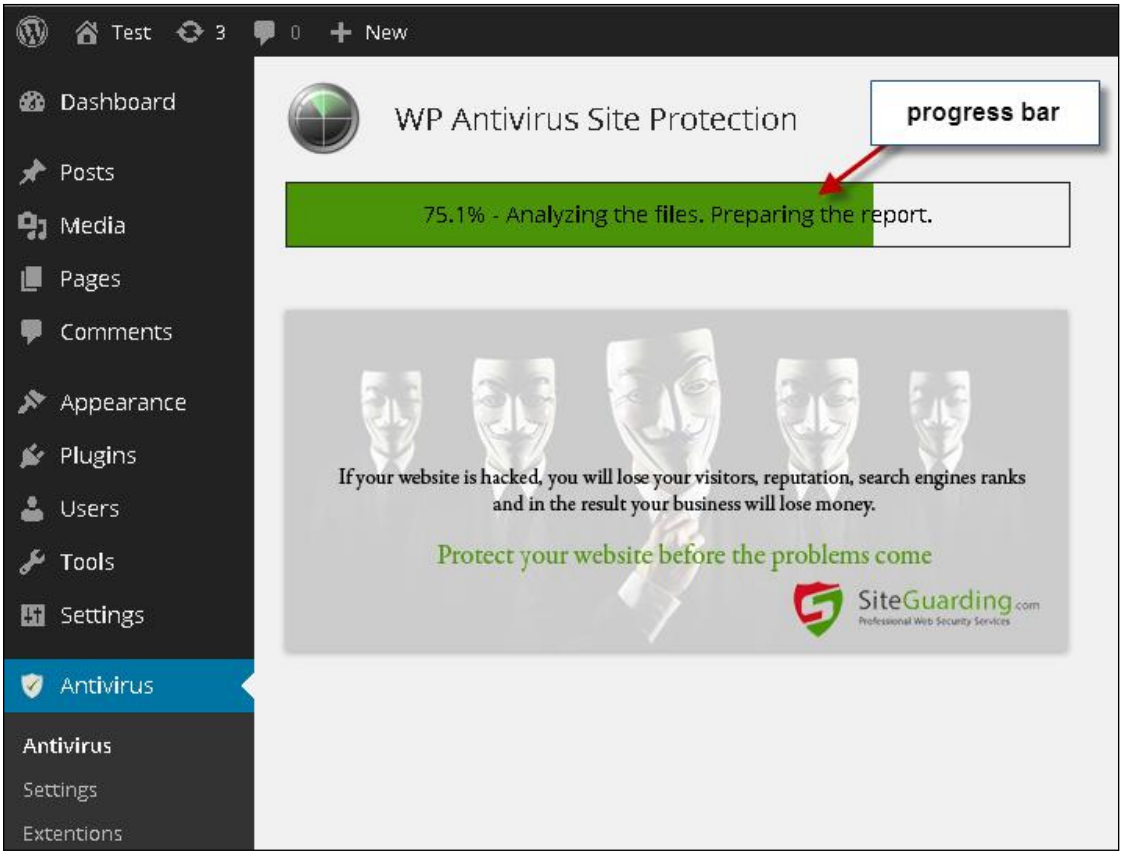
- התוסף סורק אחר בעיית HeartBleed (זהו באג אבטחה ידוע באתרים שאינם משתמשים בבפרוטוקול TLS/SSL).
- התוסף בודק קבצים באתר שבוצע בהם שינוי, ומתריע אם בוצע שינוי שיכול לפגוע באבטחת האתר.
- כמו כן התוסף מבצע סריקות מרובות על איומים של תולעים ותוכנות זדוניות הקיימות באינטרנט, כמו כך התוסף בודק פרצות אבטחה ידועות "מאחורי הקלעים".

ניטור של התוסף

- התוסף מנטר תנוע בזמן אמת הכוללת, בוטים שונים, גולשים אמיתיים, כניסות לאתר, יציאות מהאתר ומי גלש הכי הרבה זמן באתר.
- התוסף מפקח על ההפניות DNS לשרת שלך, מבצע ניטור אם בוצע שינויים לא מורשים.

ועוד מספר רב של פונקציות שתוכלו לקרוא עליהם בעמוד של התוסף.

Wp-antivirus site protection - תוסף אנטי וירוס שגם הוא מספק סריקת מערכת מקיפה לכל התיקיות והקבצים באתר. תוסף זה בניגוד לאחרים מתמחה בעיקר בעניין הסריקה המעמיקה שלו בתוך כל קבצי האתר, ניתור אחר קבצים מיותרים ודיווח בצורה נוחה וידידותית על המלצות לשינוי בקבצים ברמת קוד על מנת לדאוג להפחית פרצות.



פיצ'רים מרכזיים:

- יוצרי התוסף טוענים שיש המון סוגים של פורצים לאתרים WordPress אבל הכי ידועים הם אלו שפורצים דרך "הזרקת" MySQL ו-JavaScript, התוסף מזהה בעיות בקוד ומתריע על פרצות שונות בקבצים אלו.
- התוסף מונע שינויים בעיצוב והתכנות האתר במקרה שבוצע פרצה לאתר.
- התוסף מזהה iFrames חבויים (iFrames - קוד HTML אשר מוטמע בתוך קוד HTML אחר), יוצרי התוסף טוענים שאם במקרה הפורץ הצליח לפרוץ את פרטי ה-FTP הפורצים בדרך כלל מכניסים Hidden iframes עם וירוס אשר מוטמע לגולשים שלך כאשר הם נכנסים לאתר.
- התוסף מזהה אם בוצע פרצה באתר אשר שולחת דרך השרת שלך ספאם, התוסף מנטר ומודיע לך היכן הקובץ PHP אשר שולח ספאם נמצא באתר שלך.

- יוצרי התוסף אומרים שהאקרים הרבה פעמים שמים באתר "עמוד פישינג" אשר משמש למגוון פעולות כגון: הפניות לא רצויות, htaccess, סוסים טרויאנים, אפשרות גישה למערכת ניהול ועוד הרבה... התוסף מזהה את עמודי פישינג ומתריע לנו עליהם.

Vaultpress - תוסף שנבנה על ידי המפתחים של WordPress. מדובר בתוסף פרימיום, בשיטת מנוי ותשלום חודשי. התוסף מאפשר לכם גיבוי על בסיס יומי. הוא גם מנסה לאתר קבצים אשר נדבקו באיומים, ובמידה ונמצאו כאלה, הוא מוחק את אותם הקבצים.

קיימים עוד תוספים רבים בשוק שחלקם מנסים לעשות הכל וחלקם יותר ממוקדים לבעיות אבטחה ספציפיות. ניתן למצוא מספר רב של תוספים גם בחינם וגם בתשלום. כמובן שחלק גדול מהתוספים בחינם, מאפשרים שימוש עד רמה מסויימת ואם תרצו להעמיק את השימוש בתוסף ולבצע באמצעותו שינוי הגדרות מתקדם יותר, הדבר יהיה כרוך בתשלום נוסף למפתחי התוסף. יש לבחור ולבחון היטב מה הצורך שלכם, לפי סוג האתר ועל סמך הנתונים שיש ברשותכם, לבחור את התוספים העדיפים עליכם. וכן, גם במקרה של תוספים, כדאי מאוד להשקיע כמה שקלים עבור תוסף איכותי שמתעדכן באופן שוטף ויוכל להעניק לכם שקט.

לסיכום

אתם יכולים לבלות שעות מול המסך, לבנות עבורכם או עבור לקוח את האתר האידיאלי, זה שדמיינתם אותו, ואז ברגע של חוסר תשומת לב של אי עדכון לגירסת WordPress האחרונה, או שימוש בתוסף שעבר זמנו וכבר לא מתעדכן, אתם עלולים למצוא את עצמכם מתמודדים מול האקר שמחרב לכם את כל מה שבניתם. הקפידו תמיד לפעול על פי נהלי האבטחה המומלצים. עדכנו גירסאות, תמחקו תוספים שאתם לא צריכים, וודאו כי חברת האחסון שומרת עליכם ומאפשרת לכם לגבות את האתר על בסיס קבוע, וחשוב יותר מכל תהיו עירניים. שנו את הכתובת דרכה נכנסים לממשק הניהול, שנו סיסמאות והחביאו את הקבצים שאתם יכולים. בסופו של יום, WordPress ושלל התוספים ידעו להעניק לכם את ההגנה המירבית ביותר, אבל אתם אלה שחייבים להגדיר כל דבר ולגרום לזה לקרות.

ובנינו אם אתם רוצים לדאוג לאבטחת האתר WordPress שלכם בצורה הטובה ביותר, תדאגו לבחור חברת אחסון אתרים אשר יש לה: Firewall, מערכת סריקת קבצים באתר וניתור אחר פרצות, אפשרות לכבות את עריכת הקבצים דרך הממשק ניהול של ה-WordPress ובעיקר שיתנו לכם מענה גיבוי לכל האתר.

המאמר נכתב על ידי שחר מחברת PRM - יחסי ציבור, שיווק תוכן וקידום אתרים, תודה רבה על תרומת ידע רב למטרת כתיבת המאמר לדייב מחברת UPRESS אחסון אתרים.