מבדק חדירות

אתר עולים על מדים

צוות אבטחת מידע

יולי, 2015

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

תוכן עניינים

1. מאפייני מסמך 3
2. כללי 4
   2.1. הקדמה 4
   2.2. תיאור המערכת 4
   2.3. סיכום ממצאים טכניים 4
3. סיכום התוצאות 5
4. ממצאים 6
   4.1. *Session מיושם בצורה לא מאובטחת* 7
   4.2. שימוש ב- SSL לא מאובטח 8
   4.3. ניהול ה- Cookies במערכת לקוי 9
   4.4. לא קיימת הגנה מפני התקפת Clickjacking 10
   4.5. שירותים לא מוקשחים חושפים מידע פנימי אודות המערכת 12

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

1. מאפייני מסמך

מחבר	אודי ברוך
מבקר	
מספר גרסה	1.0
סטטוס	
תאריך הוצאה	
שם קובץ אלקטרוני	

תשומות / הערות

שם/תפקיד	הערה (אופציונאלי)	תאריך	חתימה

היסטוריה

מ. גרסה	ת. הוצאה	מחבר	שינויים מרכזיים בגרסה
1.0	06.07.2015	אודי ברוך	דוח ראשון

הפצה

מ. גרסה	נמענים

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

2. כללי

2.1 הקדמה

מסמך זה מתאר את ממצאי בדיקת החדירות שבוצעה על מערכת עולים על מדים במהלך חודש יולי 2015, שארכו כיומיים.

הבדיקה בוצעה על ידי צוות אבטחת מידע של ממשל זמין, באמצעות בודקי חדירות מוסמכים, המיומנים בתקיפת יישומים ותשתיות.

2.2 תיאור המערכת

מערכת עולים על מדים הינה מערכת המשמשת בעיקר את המיועדים לגיוס.
באתר ניתן למצוא מידע למתגייס על כל תהליך הגיוס, שאלות ותשובות ואף מידע להורים.

2.3 סיכום ממצאים טכניים

במערכת, זוהו חולשות אבטחת מידע, המאפשרות לתוקף כלשהו מרשת האינטרנט, לממש חלק מתרחישי האיום, ובכלל זאת:

1. גורם כלשהו תוקף את משתמשי המערכת.
2. גורם כלשהו מצליח לחשוף מידע חיוני על המערכת.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

3. סיכום התוצאות

במהלך המבדק, סווגו הממצאים השונים על פי 4 רמות חומרה אשר נקבעו מראש. רמת חומרת הממצאים נקבעה על בסיס הסיכון הנשקף לארגון בעקבות מימוש החשיפה. להלן רמות החומרה:

קריטית – קיים איום מיידי לתהליכים עסקיים בארגון.

גבוהה – קיים איום ישיר לתהליכים עסקיים בארגון.

בינונית – קיים איום עקיף/חלקי לתהליכים עסקיים בארגון.

נמוכה – לא קיים איום ישיר, אך ניתן לנצל את הפגיעות כדי לבצע תקיפות נוספות.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

4. ממצאים

להלן ריכוז כלל הממצאים, שזוהו במסגרת בדיקת החדירות:

מס'	תיאור הממצא	רמת חומרה
4.1	Session מיושם בצורה לא מאובטחת	**גבוהה**
Error! Reference source not found.Error! Reference source not 2found.	שימוש ב- SSL לא מאובטח	**בינונית**
Error! Reference source not 3found.	ניהול ה- Cookies במערכת לקוי	**בינונית**
Error! Reference source not 4found.	Clickjacking	נמוכה
Error! Reference source not found.Error! Reference source not 5found.	שירותים לא מוקשחים חושפים מידע פנימי אודות המערכת	נמוכה

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

4.1. Session מיושם בצורה לא מאובטחת

רמת חומרה: גבוהה

סיווג ממצא: Configuration

תיאור הבעיה

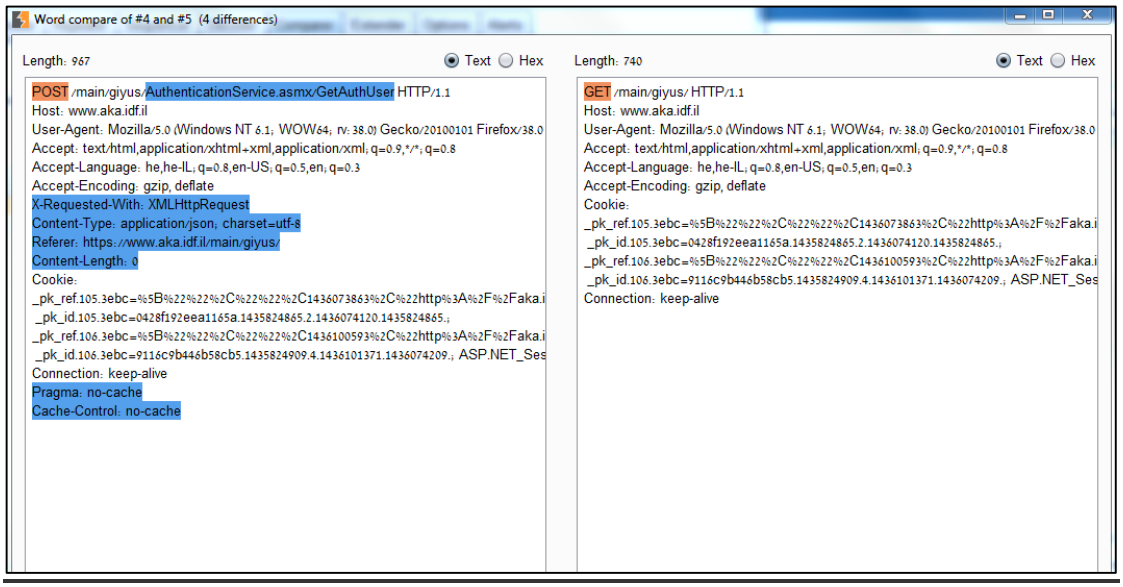
לאחר חיבור מוצלח לאפליקצייה, השרת אינו מייצר מזהה משתמש חדש (Session-ID). כתוצאה מכך, תוקף עלול לנצל זאת ולתקוף את המשתמשים גם לפני חיבורם לאפליקציה ועדיין לבצע פעולות בשמם.

פרטים טכניים

מנגנון ניהול ה-Session של האפליקציה מיושם בצורה לא תקינה. בעת התחברות לאפליקציה או התנתקות, השרת אינו מייצר מזהה עוגייה חדשה. תוקף, שמצליח לתקוף משתמש לפני התחברות מוצלחת, עשוי לקבל גישה לעוגייה ולהתחזות למשתמש.

הוכחת קיום ממצא:

על-ידי השוואת ה-Session לפני החיבור ולאחר החיבור, ניתן לראות שה- Session נשאר זהה ואינו מתחלף בחדש.



המלצות לתיקון

בעת התחברות מוצלחת לאפליקצייה, על השרת לייצר מזהה חדש באמצעות Set-Cookie.

4.2. שימוש ב- SSL לא מאובטח

רמת חומרה: ***בינונית***

סיווג ממצא: Configuration

תיאור הבעיה

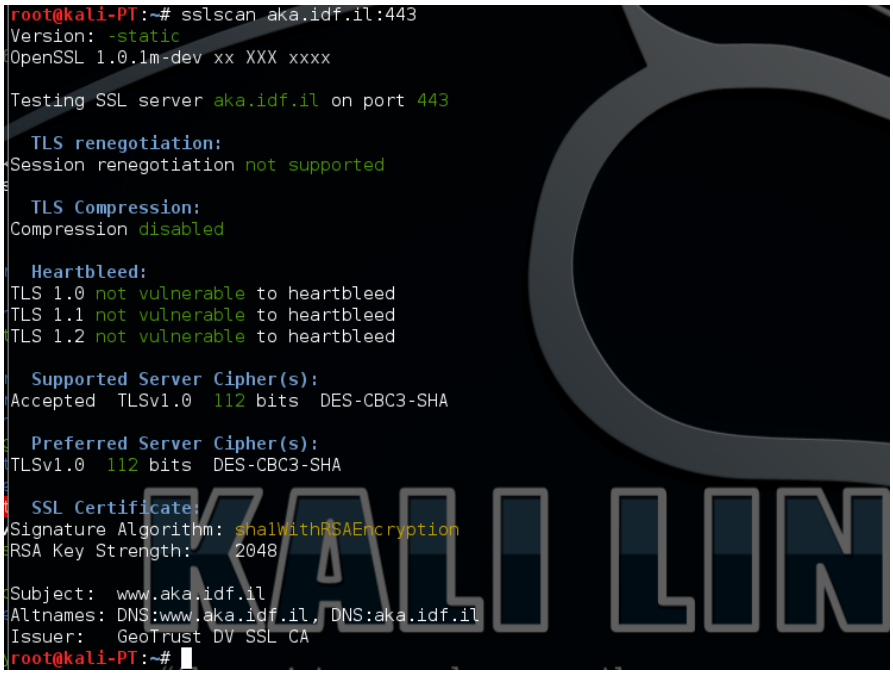
האתר עובד על גבי תווך מוצפן (HTTPS), יישום הצפנת התווך נעשה באמצעות פרוטוקולים ישנים (TLS 1.0) ואינו תומך בשימוש פרוטוקולים חדשים ומאובטחים יותר (TLS 1.2). נוסף על כך תעודת ה- SSL חתומה באמצעות אלגוריתם ישן ופגיע (SHA 1).

פרטים טכניים

שרת המערכת תומך בעבודה עם פרוטוקול TLS 1.0 בלבד שהינו פרוטוקול ישן ומכיל בעיות אבטחה. כיום (נכון לכתיבת דוח זה) הפרוטוקול המאובטח ביותר הינו TLS 1.2, שאינו נתמך כרגע בשרת כלל. בנוסף חתימת תעודת ה- SSL הינה באמצעות אלגוריתם ישן מסוג SHA1 שנחשב כיום כאינו מאובטח מספיק ומכיל בעיות אבטחה.

הוכחת קיום ממצא:

תוצאות בדיקת ה- SSL שבו נעשה שימוש באתר



המלצות לתיקון

- מומלץ ליישם את הצפנת התעבורה על גבי הפרוטוקול המאובטח ביותר שניתן כגון TLS 1.2 ולחסום את האפשרות לעבודה עם פרוטוקולים ישנים יותר.
- מומלץ להשתמש באלגוריתם מאובטח יותר בתעודת ה- SSL כגון SHA 2.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

4.3 ניהול ה- Cookies במערכת לקוי

רמת חומרה: ***בינונית***

סיווג ממצא: *Configuration*

תיאור הבעיה

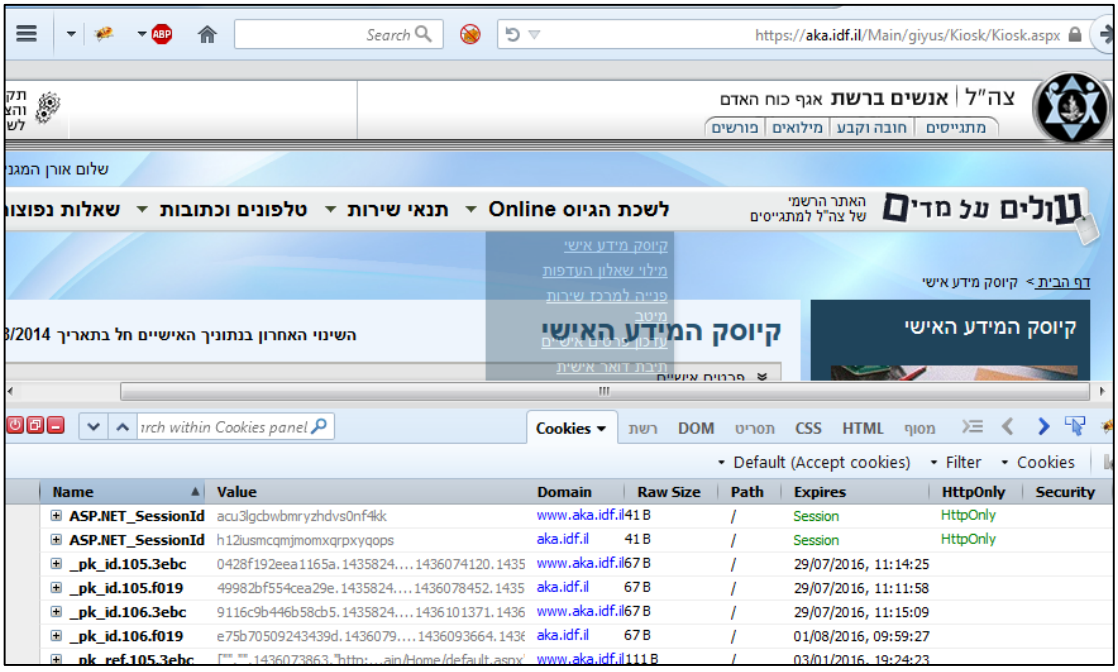
המערכת אינה מגנה כנדרש על מזהה ה- Session הייחודי של משתמשי המערכת הנמצא ב- cookie ומאפשרת לתוקף לגנוב אותו על גבי תווך לא מוצפן. לאחר שהתוקף משיג ה- cookie של המשתמש ועל ידי כך את ה- Session-ID של משתמש הוא יוכל להתחזות באופן מוחלט לאותו משתמש.

פרטים טכניים

לאחר כניסה ראשונית למערכת, השרת מספק למשתמש מזהה ייחודי (Session ID) הנשמר ב- Cookies כדי למנוע כניסה מחודשת ושמירת נתונים במהלך השימוש באתר. בעת קביעת ה- Cookie על ידי השרת (Set-Cookie) לא הוגדר פרמטר ה- Secure במאפייני העוגייה מה שמורה על הדפדפן לא לאפשר שימוש ב- cookie ללא תווך מוצפן.

הוכחת קיום ממצא:

קבלת Cookie ללא פרמטר ה- secure



המלצות לתיקון

כדי למנוע את האפשרות לגניבת ה- Session יש להגדיר את מאפייני ה- secure עבור ה- cookies המתקבלים מהשרת.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

4.4 לא קיימת הגנה מפני התקפת Clickjacking

רמת חומרה: ***נמוכה***

סיווג ממצא: *Configuration*

תיאור הבעיה

במהלך המבדק נמצא כי בכותרות המתקבלות מהשרת לא קיימת הגדרה המורה על הדפדפן לבצע הגנה מפני הצגת תוכן באתר מרוחק (iframe) מה שחושף את משתמשי האתר להתקפות מסוג Phishing ו – Clickjacking היות וניתן להציג תכנים של אתר הגיוס באתרים מרוחקים ללא כל חסימה מצד הדפדפן. יש לציין כי הגדרות למניעת התקפות מסוג זה מגיעות מהשרת והחסימה בפועל מבוצעת בדפדפן שבצד הלקוח.

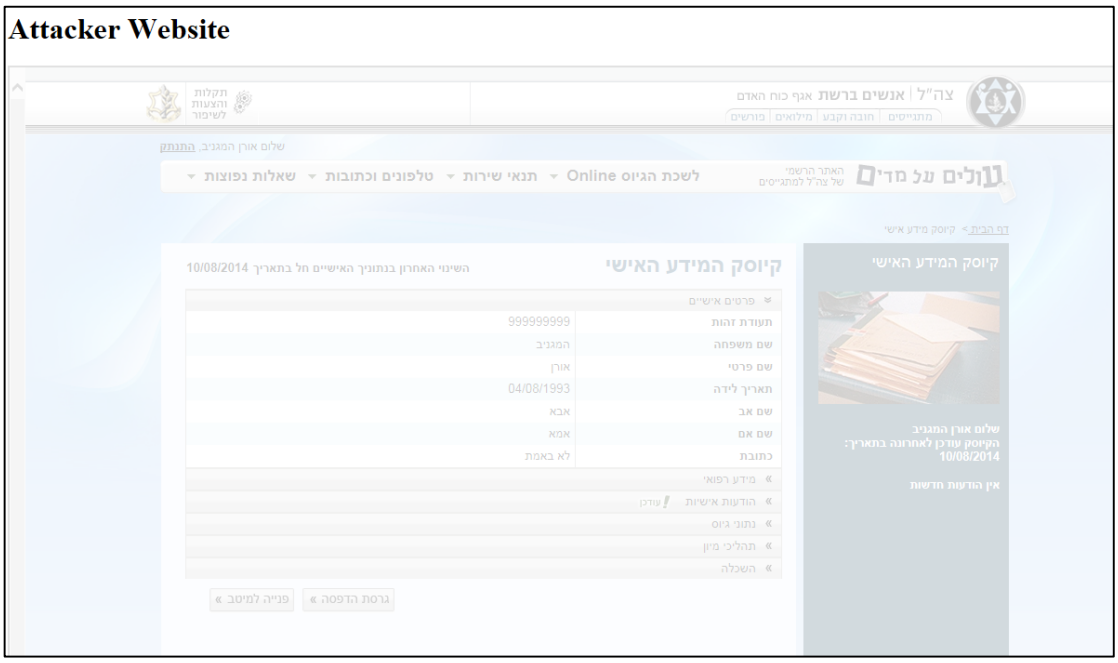
פרטים טכניים

כאשר גולשים לאתר גיוס מתקבלות כותרות מצד השרת אל הדפדפן של הגולש ולפיהן הדפדפן מבצע פעולות שונות בצד הלקוח.

ניתן לראות כי לא מתקבלות כותרות המורות על הדפדפן לבצע הגנה מפני Clickjacking, כגון –X-Frame-Options: deny , ולכן במצב זה ניתן להציג תכנים של אתר גיוס באתר מרוחק ולבצע הונאות שונות למשתמשי האתר באתרים זדוניים.

הוכחת קיום ממצא:

דוגמא 1: הצגת תכנים של אתר גיוס באתר מרוחק



המלצות לתיקון

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

- יש להגדיר בכותרות שרת ה- IIS את הגדרת ה- X-Frame, בהגדרה זו ניתן לבחור בין אם לאפשר הצגת תכנים תחת אותו דומיין במיקומים שונים בו או לחלופין לחסום זאת לכולם. להלן אפשרויות ההגדרה:

חסימה לגמרי – DENY

מאופשר לאותו דומיין – SAMEORIGIN

מאופשר לכתובת ספציפית - ALLOW-FROM

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

4.5 שירותים לא מוקשחים חושפים מידע פנימי אודות המערכת

רמת חומרה: נמוכה

סיווג ממצא: *Data Exposure*

תיאור הבעיה

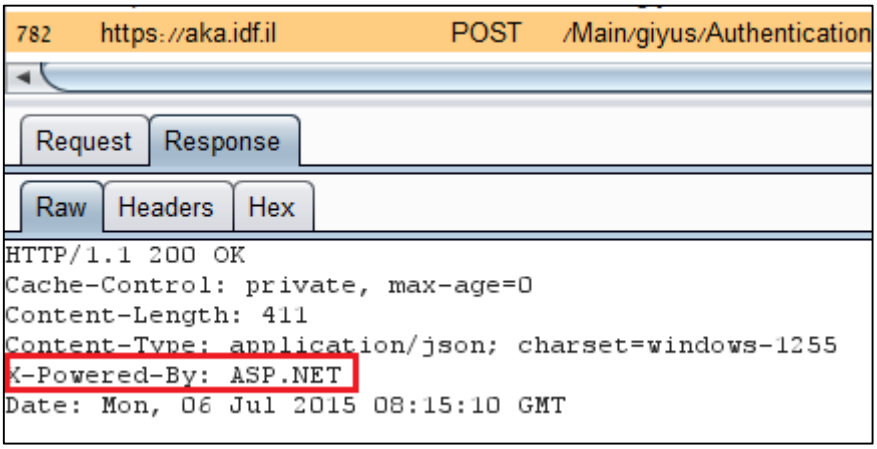
המערכת חושפת מידע אודות התשתית בה היא מאוחסנת כגון פלטפורמת הפיתוח, גרסת ASP.NET וכו'. חשיפת מידע זה מאפשרת לגורם זדוני לאסוף מידע חיוני על המערכת ולמקד את התקפתם. חשיפת המידע עוזרת לתוקפים למצוא פגיעויות ידועות או חדשות אשר קיימות או יימצאו במערכת.

פרטים טכניים

בעת ביצוע פעולות באתר, הכותרות החוזרות לצד המשתמש חושפות מידע אודות גרסת המערכת.

הוכחת קיום ממצא:

זיהוי גרסת המערכת



המלצות לתיקון

- יש להקשיח את שרת ה- IIS כך שלא יחשוף את גרסתו ואת הגרסאות של המודולים המותקנים בו.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין