מבדק חדירות

אתר השכר והכספים

צוות אבטחת מידע

מאי, 2015

תוכן עניינים

Contents

1. מאפייני מסמך

מחבר	אודי ברוך
מבקר	
מספר גרסה	1.0
סטטוס	
תאריך הוצאה	31.05.2015
שם קובץ אלקטרוני	

תשומות / הערות

שם/תפקיד	הערה (אופציונאלי)	תאריך	חתימה

היסטוריה

מ. גרסה	ת. הוצאה	מחבר	שינויים מרכזיים בגרסה
1.0	31.05.2015	אודי ברוך	דו"ח ראשון

הפצה

מ. גרסה	נמענים
טיוטה להתייחסות	

2. הקדמה

2.1 הקדמה

מסמך זה מתאר את ממצאי בדיקת החדירות שבוצעה על אתר השכר והכספים במהלך חודש מאי 2015, שארכו כשלושה ימים.

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

2.2 תיאור המערכת

אתר השכר והכספים מאפשר רישום של משתמשים וגישה לתלושי השכר און ליין.
https://aka.idf.il/Main/Sachar/

2.3 סיכום ממצאים טכניים

במערכת זוהו חולשות אבטחת מידע המאפשרות לתוקף כלשהו מרשת האינטרנט לתקוף את המערכת ומשתמשיה:

1. ניהול Session בצורה לא תקינה.
2. סיסמאות נשמרות בבסיס הנתונים בצורה לא מוצפנת.
3. חשיפת מדיע טכנולוגי על המערכת.

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.
להן 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.

4. ממצאים

להלן ריכוז כלל הממצאים, שזוהו במסגרת בדיקת החדירות:

מס'	תיאור הממצא	רמת חומרה
4.11	Session מיושם בצורה לא מאובטחת	***גבוהה***
Error! Reference source not 2found.	Cookie מיושם בצורה לא מאובטחת	**בינונית**
Error! Reference source not 3found.	סיסמאות נשמרות בבסיס הנתונים בצורה לא מוצפנת	**בינונית**
4.54	מיפוי משתמשי המערכת	***נמוכה***
4.65	Click-Jacking	***נמוכה***
Error! Reference source not 6found.	שרתים לא מוקשחים חושפים מידע פנימי אודות המערכת	***נמוכה***
4.7	נעילת משתמש D.o.S (מניעת שירות)	***הערה***
0	שחזור סיסמא D.o.S (מניעת שירות)	***הערה***

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.

המלצות לתיקון

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

4.2. ***סיסמאות נשמרות בבסיס הנתונים בצורה לא מוצפנת***

רמת חומרה: בינונית

סיווג ממצא: Confidential Data Stored in Clear Text in Database

תיאור הבעיה

בתהליך שחזור הסיסמא, האפליקציה שולחת את הסיסמא לתיבת הדואר של המשתמש. חשיפה זו מאפשרת לפורץ פוטנציאלי לאתר את הסיסמאות הנשלחות למשתמש באמצעות חדירה לתיבת הדואר שלו או באמצעות ציתות לתעבורה של תיבה שאינה מוצפנת ולהזדהות בשמו לאפליקציה.

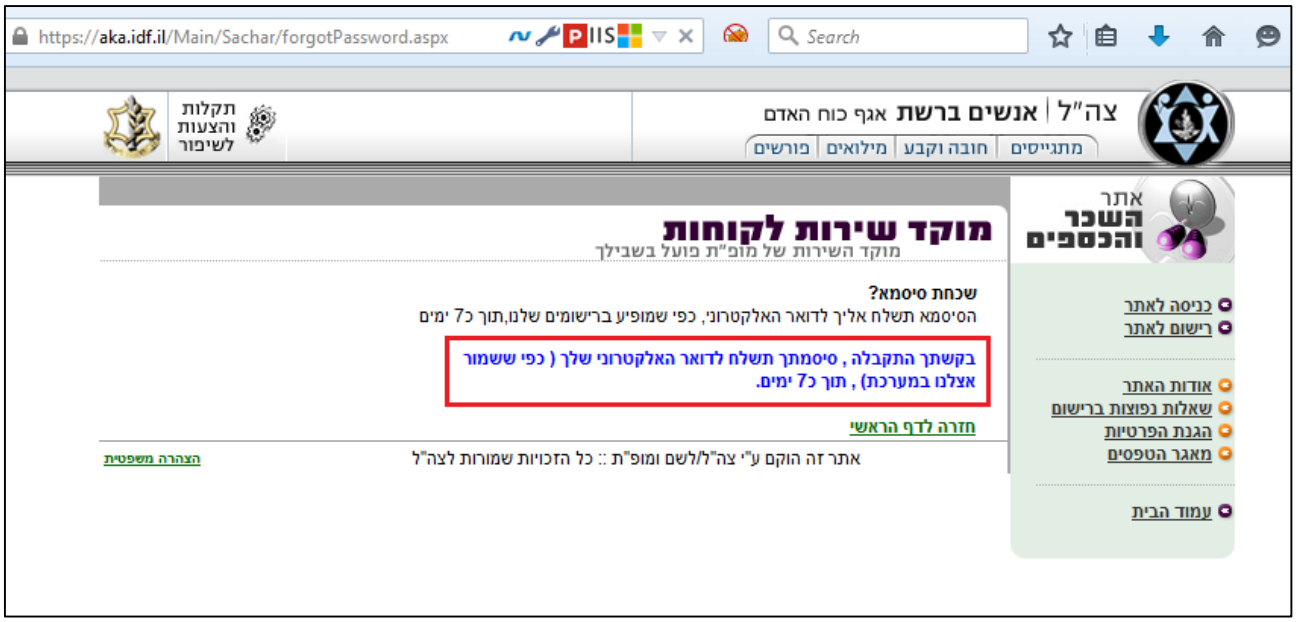
בנוסף, הדבר מעיד על אכסון לא מאובטח של הסיסמאות בבסיס הנתונים אשר יאפשר לתוקפים לשחזר את מידע הסיסמאות במידה והשיגו גישה כלשהי למידע זה.

פרטים טכניים

נמצא כי סיסמאות המשתמשים נשמרות בצורה לא מאובטחת בבסיס הנתונים. נהוג לאכסן סיסמאות משתמשים תוך שימוש בפעולה מתמטית חד-כיוונית (HASH) המופעלת על סיסמת המשתמש ועל ערך רנדומלי ייחודי המיוצר עבור כל משתמש (SALT). צורה זו של איכסון אינה מאפשרת שיחזור של הסיסמאות במידה ותוקף השיג גישה למידע המאוכסן בבסיס הנתונים.

הוכחת קיום ממצא:

בעת תהליך שחזור סיסמא קיבלנו את ההודעה הבאה:



מאחר וזמן ההמתנה לקבלת הסיסמא ארוך מהרגיל, ניתן להסיק מההודעה שהתקבלה את אופן שמירת הסיסמא.

המלצות לתיקון

- בתהליך שחזור הסיסמא לא צריכה להישלח הסיסמא חזרה לתיבת הדואר של המשתמש. לחילופין, משתמש המבקש לאחזר את סיסמתו צריך לקבל דואר עם מפתח שחזור ייחודי וחד פעמי ללא שם המשתמש. המשתמש יוכל להכניס את המפתח הזה במסך ההזדהות (או במסך שחזור סיסמא שייועד לכך) ולאחר שיקיש את המפתח יופנה למסך שחזור סיסמא, בו הוא יצטרך להשיב על שאלה סודית (כמו לדוגמא: מה היה שם נעוריה של אמך?) ולאחר מכן הוא יוכל לשנות את סיסמתו.
- בנוסף יש לאכסן את סיסמאות המשתמשים בבסיס הנתונים תוך שימוש בפונקצית HASH וערך SALT אשר יבטיח כי לא יהיה ניתן לשחזר את הנתונים הרגישים (ערך ה- SALT הינו ערך רנדומלי בן 16 תווים אשר ייוצר עבור המשתמש בעת יצירתו ויאוכסן בבסיס הנתונים לצד פרטי המשתמש).

4.3. Cookie מיושם בצורה לא מאובטחת

רמת חומרה: בינונית

סיווג ממצא: Configuration

תיאור הבעיה

המערכת אינה מגנה על מזהה ה- Session הייחודי של משתמשי המערכת ומאפשרת לתוקף לגנוב אותו בצורות שונות. לאחר שהתוקף משיג Session-ID של משתמש מערכת לגיטימי הוא יוכל להתחזות באופן מוחלט לאותו משתמש, לבצע פעולות ומתקפות בשמו ובהרשאותיו. התוקף יוכל לעשות שימוש לרעה במידע שהשיג לצורך ביצוע מתקפות הונאה (Phishing) לצרכי תחרות ולשם פגיעה תדמיתית בחברה ובמערכותיה.

הוכחת הממצא:

```
HTTP/1.1 302 Found
Cache-Control: private
Content-Length: 142
Content-Type: text/html; charset=windows-1255
Location: /Main/Sachar/default.aspx
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Set-Cookie: ASP.NET SessionId=gphvgryzjokyvfdt4raf5shl; path=/; HttpOnly
Date: Wed, 27 May 2015 04:46:42 GMT
```

פרטים טכניים

לאחר הזדהות מספק שרת המערכת למשתמש מזהה ייעודי (Session ID) הנשמר ב- Cookies לצורך אימות זהות המשתמש אל מול המערכת. בעת קביעת ה- Cookie על ידי השרת (Set-Cookie) לא הוגדר מאפיין (secure) המגן על המידע הנשמר במנגנון.

המלצות לתיקון

יש לקבוע את המאפיין 'secure' עבור נתונים רגישים הנשמרים באמצעות Set-Cookie.

4.4. Click-Jacking

רמת חומרה: בינונית

סיווג ממצא: Insecure Deployment

תיאור הבעיה

אתרי צד שלישי זדוניים יכולים לגרום למשתמשי קצה לבצע פעולות במערכת ללא ידיעתם, על ידי הכללת טפסים בלתי נראים המקושרים לרכיבים ספציפיים במערכת, הסתרתם באמצעות דפי תוכן פיקטיביים ושימוש בהקשות העכבר של המשתמש על דפי תוכן אלו בכדי לבצע פעולות בדפי המערכת המקושרים לטפסים.

התקפה זו עלולה לאפשר לתוקפים מרשת האינטרנט לבצע פעולות בשם משתמשי המערכת, לאסוף מידע פרטי על משתמשי האתר, ובמקרים מסוימים אף להתחזות למשתמשים באופן מלא.

פרטים טכניים

מתקפת ClickJacking הינה מתקפת הונאה שמטרתה "לגנוב" לחיצות עכבר של משתמשי קצה תמימים על מנת לבצע מגוון של פעולות זדוניות. התקפה זו מבוצעת דרך אתר צד שלישי זדוני הנמצא בשליטה מלאה או חלקית של תוקף, בזמן שמשתמשים לגיטימיים של המערכת גולשים בו.

"גניבת" לחיצות העכבר של משתמש הקצה יאפשרו לפורץ לבצע בשם המשתמש מגוון של פעולות במערכת, ובכלל זאת כל פעולה שניתן לבצע דרך טופס או קישור.

הוכחת הממצא:

<u>המלצות לתיקון</u>

ישנן מספר דרכים מומלצות להתמודדות עם חשיפה זו במערכת, ובמידת האפשר, מומלץ לממש את כולן.

שילוב של מספר טכניקות Anti-ClickJacking:

- מניעת קישור של דפים באתר לפקדי Frame ע"י קוד JavaScript ייעודי המבצע פעולה בשם Frame Busting. להלן דוגמת קוד ב-Javascript:

```
<script>
if (top!=self)
    top.location.href=self.location.href;
</script>
```

- שימוש ב- HTTP Response Header בשם X-FRAME-OPTIONS, אשר מונע מדפים להיות ממוקמים בתוך Frame (נתמך בעיקר בדפדפנים חדשים). להלן שני הערכים הניתנים להגדרה ב-Header:
  - DENY – מונע מהדף להיות מוצג בתוך Frame באופן גורף.
  - SAMEORIGIN – מונע מהדף להיות מוצג בתוך Frame במידה ורכיב ה-Frame המקושר אליו אינו מאותו Domain (מומלץ כברירת מחדל, במקום הפתרונות האחרים בסעיף 1, ובמיוחד בדפים שאמורים להיות מוצגים בתוך FRAME פנימי באתר). יש לציין כי פתרון זה נתמך על ידי דפדפני Internet Explorer מגרסא 8 ומעלה (אך בעתיד, עשוי להיתמך על ידי דפדפנים נוספים). להלן דוגמת קוד (מתאים לשפות C# ו-JAVA):

```
// sample code for completely preventing framing of this content
response.addHeader( "X-FRAME-OPTIONS", "DENY" );
// sample code for enabling content framing only from the same domain
response.addHeader( "X-FRAME-OPTIONS", "SAMEORIGIN" );
```

יישום מנגנון טוקניזציה:

ניתן להתמודד עם ההתקפה על ידי הטמעה של מנגנון הגנה מהתקפות CSRF כאשר המנגנון ימומש כך שיחלוש על כלל הדפים הפנימיים במערכת (מלבד דף ה-Login), וזאת בכדי לאפשר לו להתמודד גם עם התקפות ClickJacking.

כדי להקטין את הסיכון מהתקפות הונאה, בנוסף למאפיינים הרגילים של מנגנון זה, במקרה וה - AntiCSRF Token אשר התקבל מצד המשתמש אינו תקין, יש לנתק את המשתמש מהמערכת באופן יזום.

4.5. מיפוי משתמשים

רמת חומרה: נמוכה

סיווג ממצא: Configuration

תיאור הבעיה

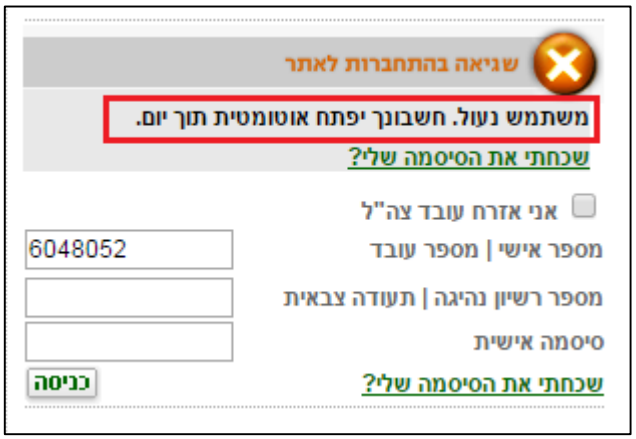
פורצים יכולים לנצל את הבדלי התשובות במנגנון ההזדהות בכדי לאתר שמות משתמשים הקיימים במערכת, איתור שמות המשתמשים יאפשר לפורצים לבצע נסיונות התחברות ע"י ניחוש סיסמאות.

פרטים טכניים

בכדי להזדהות בפני המערכת, על המשתמש להזין מספר תעודת זהות וסיסמא. המערכת מציגה הודעת שגיאה שונה במידה והתעודת זהות אינה קיימת במערכת. ההבדלים בהודעות השגיאה מאפשרים לפורץ המבצע התקפות Brute-Force להסיק אילו מתעודות הזהות קיימות במערכת ואילו לא.

הוכחת הממצא:

בעת נעילת המשתמש מופיעה ההודעה הבאה:



המלצות לתיקון

יש להציג הודעת שגיאה אחידה, ללא קשר לסיבת כשלון ההזדהות.

4.6 חשיפת שרת האפליקציה

רמת חומרה: נמוכה

סיווג ממצא: Fingerprinting

תיאור הבעיה:

כברירת מחדל, שרת הרשת חושף את גרסתו וסוגו. מידע זה יעיל ביותר עבור תוקפים, אשר יכולים לחפש ברשת פגיעויות ידועות ומוכרות עבור אותו סוג שרת ולנצל אותם על מנת לפרוץ אל השרת.

פרטים טכניים:

שרת האפליקציה חושף מידע רגיש, כגון סוג השרת.

הערה: פגיעות זאת נמצאה במספר מקומות באפליקציה ולכן צריך לטפל בה בכל המקומות בהן היא מופיעה, ולא רק בדוגמאות המופיעות בממצא זה.

הוכחת הממצא:

ניתן לראות כי סוג שרת הרשת וגרסתו נחשפים ב-headers המוחזרים משרת האפליקציה.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 26876
Content-Type: text/html; charset=windows-1255
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Date: Tue, 26 May 2015 13:56:23 GMT
```

המלצות לתיקון:

יש להסיר את סוג וגרסת השרת מה-HTTP Headers.

4.7. נעילת משתמש D.o.S (מניעת שירות)

רמת חומרה: הערה

סיווג ממצא: D.o.S

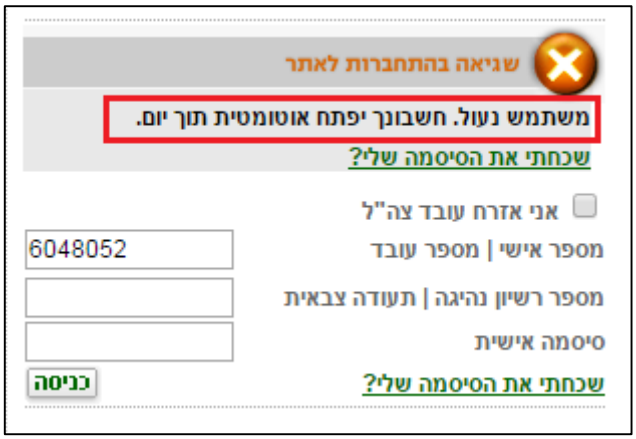
תיאור הבעיה:

בעת ריבוי נסיונות התחברות למערכת ללא הצלחה, המערכת נועל את המשתמש על מנת למנוע נסיון פריצה לחשבון.
זהו פתרון טוב למנוע נסיון פריצה, עם זאת המערכת נועל את המשתמש ליום שלם ולכן מונעת ממנו שירות לזמן רב.

פרטים טכניים:

לאחר מספר נסיונות התחברות לא מוצלחים המערכת מבצעת נעילה למשתמש למשך יום ומונעת ממנו קבלת שירות.

הוכחת הממצא:



המלצות לתיקון:

יש לשחרר את המשתמש מנעילה לאחר 20 דקות.

4.8. ***שחזור סיסמא D.o.S (מניעת שירות)***

רמת חומרה: הערה

סיווג ממצא: D.o.S

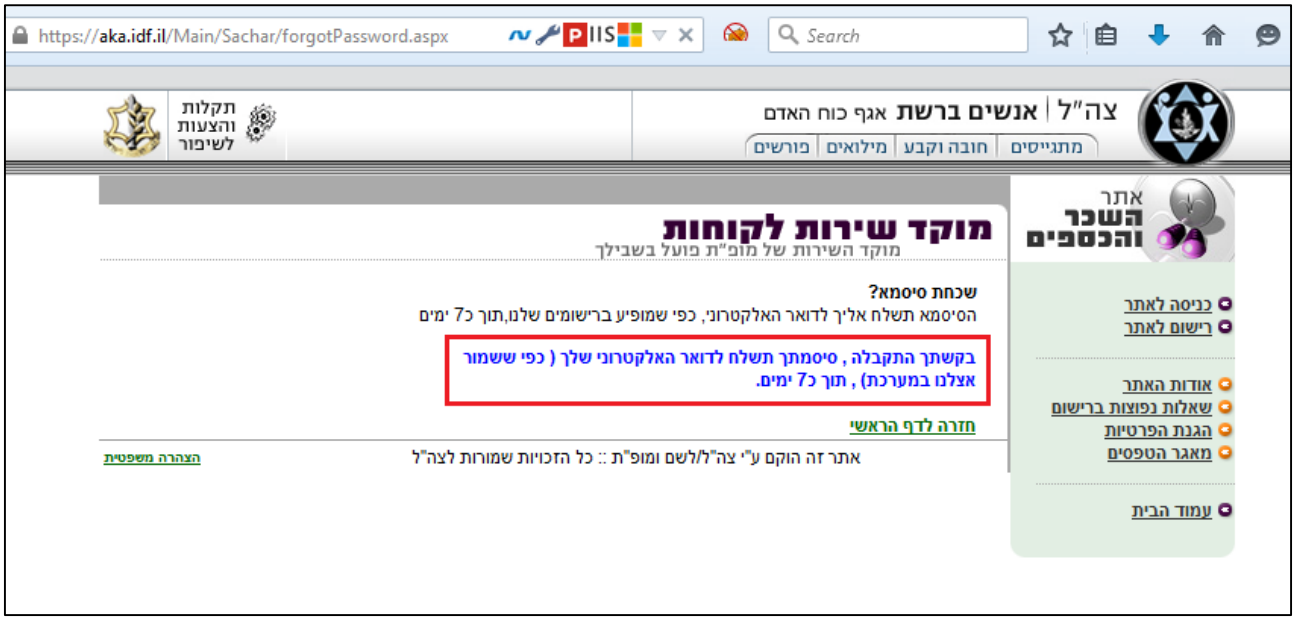
תיאור הבעיה:

בעת נסיון שחזור סיסמא, המערכת מודיעה כי זמן לשחזור הוא תוך כ-7 ימים.
ולפי כך מנגנון שחזור הסיסמא משבית את המשתמש ומונע ממנו שירות למשך 7 ימים.

פרטים טכניים:

מנגנון שחזור סיסמא מונע שירות מהמשתמש למשך 7 ימים.

הוכחת הממצא:



המלצות לתיקון:

יש לשחזר סיסמא באופן מיידי ע"י שימוש במנגנון שחזור סיסמא תקין (בהתאם להמלצות בסעיף 4.2).