

# מבדק חדירות

## אתר עולים על מדים



### צוות אבטחת מידע

יולי, 2015

## תוכן עניינים

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

# 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

## 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.

### 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.

## 4. ממצאים

להלן ריכוז כלל הממצאים, שזוהו במסגרת בדיקת החדירות:

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

## 4.1. Session מיושם בצורה לא מאובטחת

רמת חומרה: **גבוהה**

**סיווג ממצא: Configuration**

### תיאור הבעיה

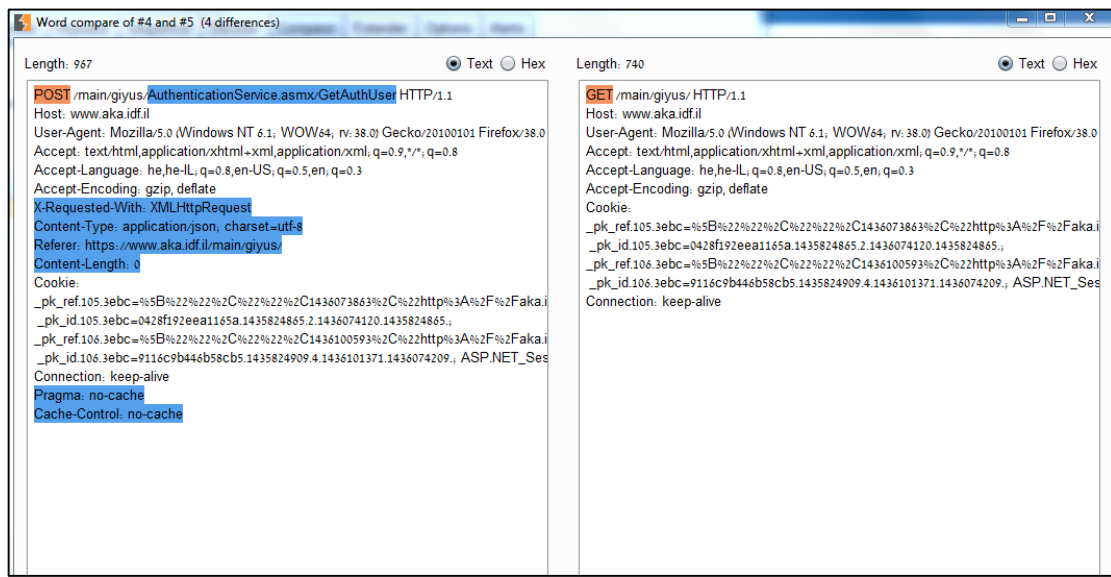
לאחר חיבור מוצלח לאפליקציה, השרת אינו מייצר מזהה משתמש חדש (Session-ID). כתוצאה מכך, תוקף עלול לנצל זאת ולתקוף את המשתמשים גם לפני חיבורם לאפליקציה ועדיין לבצע פעולות בשמם.

### 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 לאפליקציה, 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

```

root@kali-PT:~# sslscan aka.idf.il:443
Version: -static
OpenSSL 1.0.1m-dev xx XXX xxxx

Testing SSL server aka.idf.il on port 443

  TLS renegotiation:
  Session renegotiation not supported

  TLS Compression:
  Compression disabled

  Heartbleed:
  TLS 1.0 not vulnerable to heartbleed
  TLS 1.1 not vulnerable to heartbleed
  TLS 1.2 not vulnerable to heartbleed

  Supported Server Cipher(s):
  Accepted TLSv1.0 112 bits DES-CBC3-SHA

  Preferred Server Cipher(s):
  TLSv1.0 112 bits DES-CBC3-SHA

  SSL Certificate:
  Signature Algorithm: sha1withRSAEncryption
  RSA Key Strength: 2048

  Subject: www.aka.idf.il
  Altnames: DNS:www.aka.idf.il, DNS:aka.idf.il
  Issuer: GeoTrust DV SSL CA
root@kali-PT:~#

```

### 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.



## 4.3. ניהול ה- Cookies במערכת לקוי

רמת חומרה: **בינונית**

סיווג ממצא: **Configuration**

### תיאור הבעיה

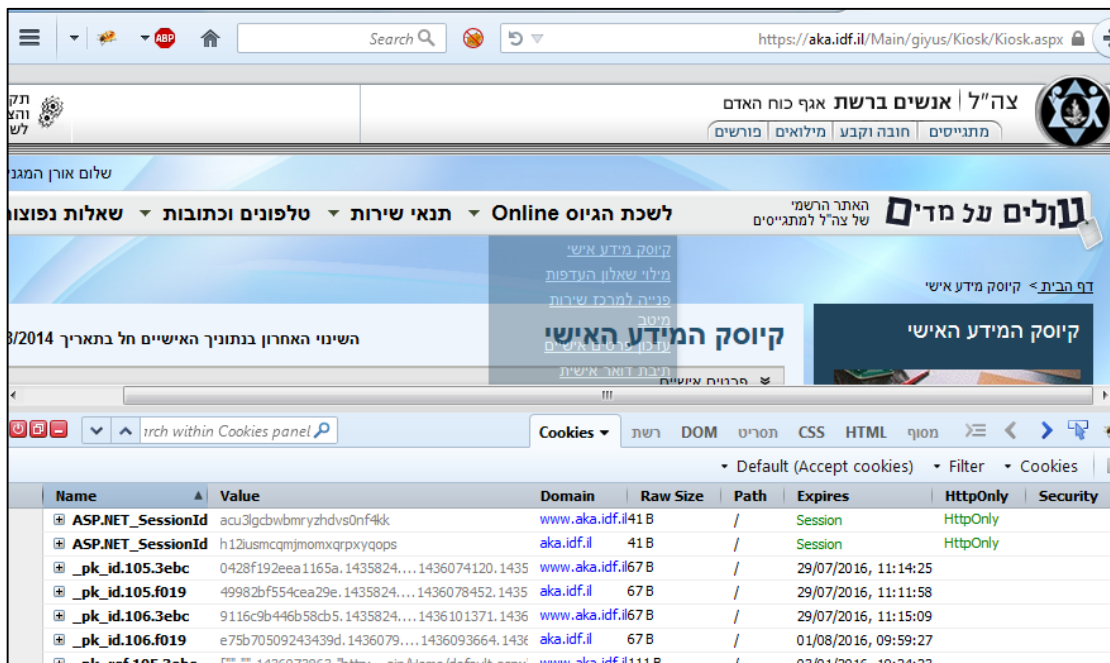
המערכת אינה מגנה כנדרש על מזהה ה- Session הייחודי של משתמשי המערכת הנמצא ב- cookie ומאפשרת לתוקף לגנוב אותו על גבי תווך לא מוצפן. לאחר שהתוקף משיג ה- cookie של המשתמש ועל ידי כך את ה- Session-ID של משתמש הוא יוכל להתחזות באופן מוחלט לאותו משתמש.

### 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**



Name	Value	Domain	Raw Size	Path	Expires	HttpOnly	Security
ASP.NET_SessionId	acu3lgbwbmryzhdvs0nf#kk	www.aka.idf.il	41 B	/	Session	HttpOnly	HttpOnly
ASP.NET_SessionId	h12usmcqnmjomaxqpxyqops	aka.idf.il	41 B	/	Session	HttpOnly	HttpOnly
_pk_id.105.3ebc	0428f192eea1165a.1435824....1436074120.1435	www.aka.idf.il	67 B	/	29/07/2016, 11:14:25		
_pk_id.105.f019	49982bf554cea29e.1435824....1436078452.1435	aka.idf.il	67 B	/	29/07/2016, 11:11:58		
_pk_id.106.3ebc	9116c9b446b58cb5.1435824....1436101371.1436	www.aka.idf.il	67 B	/	29/07/2016, 11:15:09		
_pk_id.106.f019	e75b70509243439d.1436079....1436093664.1436	aka.idf.il	67 B	/	01/08/2016, 09:59:27		
_nk_ref.105.3ebc	[redacted]	www.aka.idf.il	111 B	/	03/01/2016, 19:24:23		

### 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.

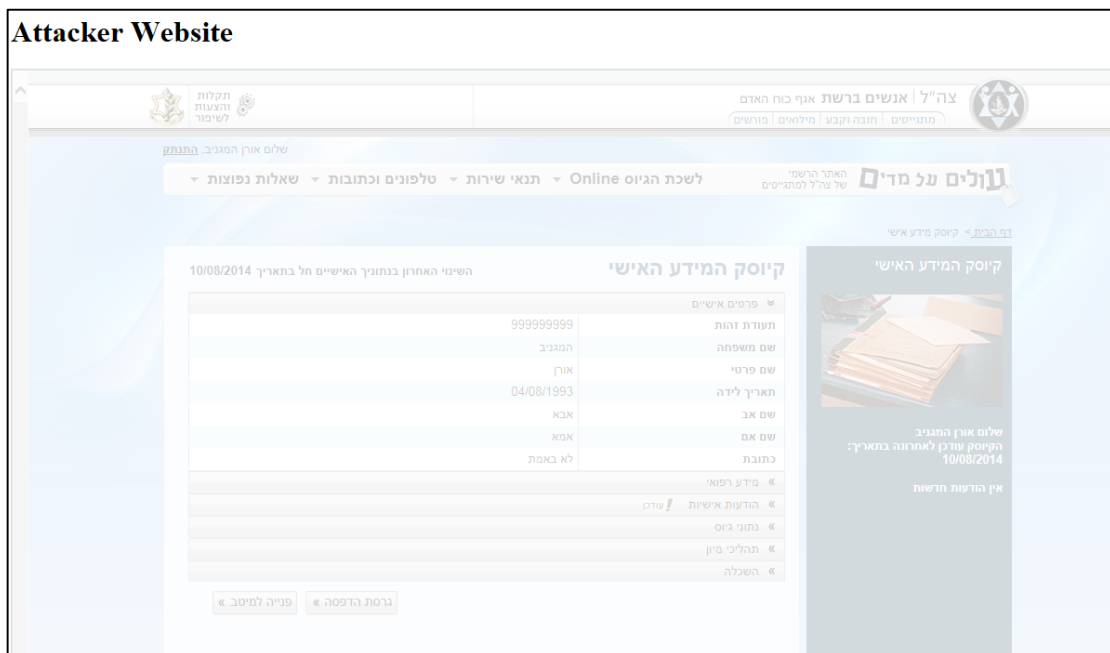
### פרטים טכניים

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**



The screenshot shows a web page titled "Attacker Website" with a header containing the Israeli government logo and navigation links. The main content area features a form titled "קיוסק המידע האישי" (Personal Information Kiosk) with the following fields:

פרטים אישיים	999999999
תעודת זהות	המגזב
שם משפחה	אורן
שם פרטי	04/08/1993
תאריך לידה	אבא
שם אב	אמא
שם אם	לא באמת
כתובת	
מידע רפואי	
הודעות אישיות	
נתיב גיוס	
תלמידי מיון	
השגלה	

Below the form are buttons for "גרסת הדפסה" (Print Version) and "פנייה למיטב" (Contact Us). On the right side of the page, there is a sidebar with a heading "קיוסק המידע האישי" and a sub-heading "שלים אופן המגזב" (Complete the form).

### 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

מאפשר לאותו דומיין – SAMEORIGIN

מאפשר לכתובת ספציפית - ALLOW-FROM

## 4.5. שירותים לא מוקשחים חושפים מידע פנימי אודות המערכת

רמת חומרה: **נמוכה**

סיווג ממצא: **Data Exposure**

תיאור הבעיה

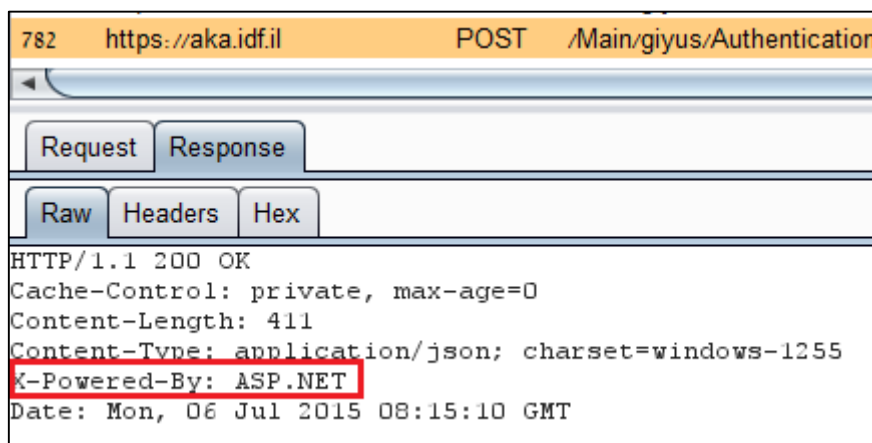
המערכת חושפת מידע אודות התשתית בה היא מאוחסנת כגון פלטפורמת הפיתוח, גרסת ASP.NET וכו'. חשיפת מידע זה מאפשרת לגורם זדוני לאסוף מידע חיוני על המערכת ולמקד את התקפתם. חשיפת המידע עוזרת לתוקפים למצוא פגיעויות ידועות או חדשות אשר קיימות או יימצאו במערכת.

פרטים טכניים

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

הוכחת קיום ממצא:

זיהוי גרסת המערכת



```

782 https://aka.idf.il POST /Main/giyus/Authentication
Request Response
Raw Headers Hex
HTTP/1.1 200 OK
Cache-Control: private, max-age=0
Content-Length: 411
Content-Type: application/json; charset=windows-1255
X-Powered-By: ASP.NET
Date: Mon, 06 Jul 2015 08:15:10 GMT

```

המלצות לתיקון

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