# מבדק חדירות

## אתר הרבנות הצבאית


**צוות אבטחת מידע**

**יולי, 2015**

# תוכן עניינים

# 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 | 05.07.2015 | אודי ברוך | דוח ראשון |
| | | | |
| | | | |
| | | | |

### הפצה

| מ. גרסה | נמענים |
|---|---|
| | |
| | |
| | |
| | |

# 2. כללי

## 2.1 הקדמה

מסמך זה מתאר את ממצאי בדיקת החדירות שבוצעה על אתר הרבנות 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

באתר הרבנות ניתן למצוא שיעורי דת, תפילות, הלכות וכ'ו.

## 2.3 סיכום ממצאים טכניים

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

1. גורם כלשהו מצליח לחשוף מידע חיוני על המערכת.

***הערה:*** יש לציין שעמוד צור קשר באתר אינו קיים (לינק שבור), לכן עמוד זה לא יכל להיבדק ויש לשים לב לזה בעת חזרתו לפעילות.

# 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:

| מס' | תיאור הממצא | רמת חומרה |
|---|---|---|
| 4.1 | שירותים לא מוקשחים חושפים מידע פנימי אודות המערכת | *נמוכה* |
| 4.1 | Clickjacking | *נמוכה* |

## 4.1 שירותים לא מוקשחים חושפים מידע פנימי אודות המערכת

***רמת חומרה: נמוכה***

***סיווג ממצא:*** *Data Exposure*

***תיאור הבעיה***

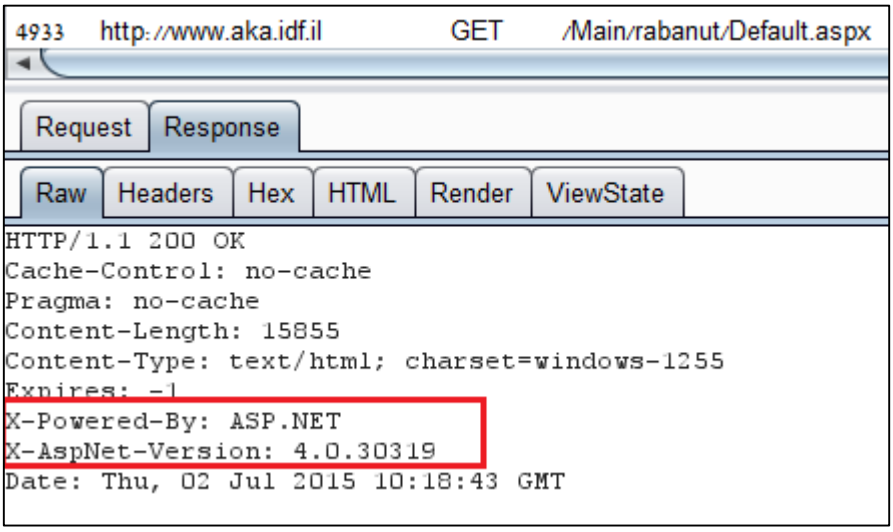
המערכת חושפת מידע אודות התשתית בה היא מאוחסנת כגון פלטפורמת הפיתוח, גרסת ASP .NET וכו'. חשיפת מידע זה מאפשרת לגורם זדוני לאסוף מידע חיוני על המערכת ולמקד את התקפתם. חשיפת המידע עוזרת לתוקפים למצוא פגיעויות ידועות או חדשות אשר קיימות או יימצאו במערכת.

***פרטים טכניים***

בעת ביצוע פעולות באתר, הכותרות החוזרות לצד המשתמש חושפות מידע אודות גרסת ה-ASP.NET בה המערכת עובדת, גרסת פלטפורמת (גרסה 4.0.30319).

***הוכחת קיום ממצא:***

***ניתן לראות שהמערכת חושפת את גרסת ASP.NET***




***המלצות לתיקון***

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

## 4.2 לא קיימת הגנה מפני התקפות "חטיפת קליקים" (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 הרבנות באתרים מרוחקים ללא כל חסימה מצד הדפדפן. יש לציין כי הגדרות למניעת התקפות מסוג זה מגיעות מהשרת והחסימה בפועל מבוצעת בדפדפן שבצד הלקוח.

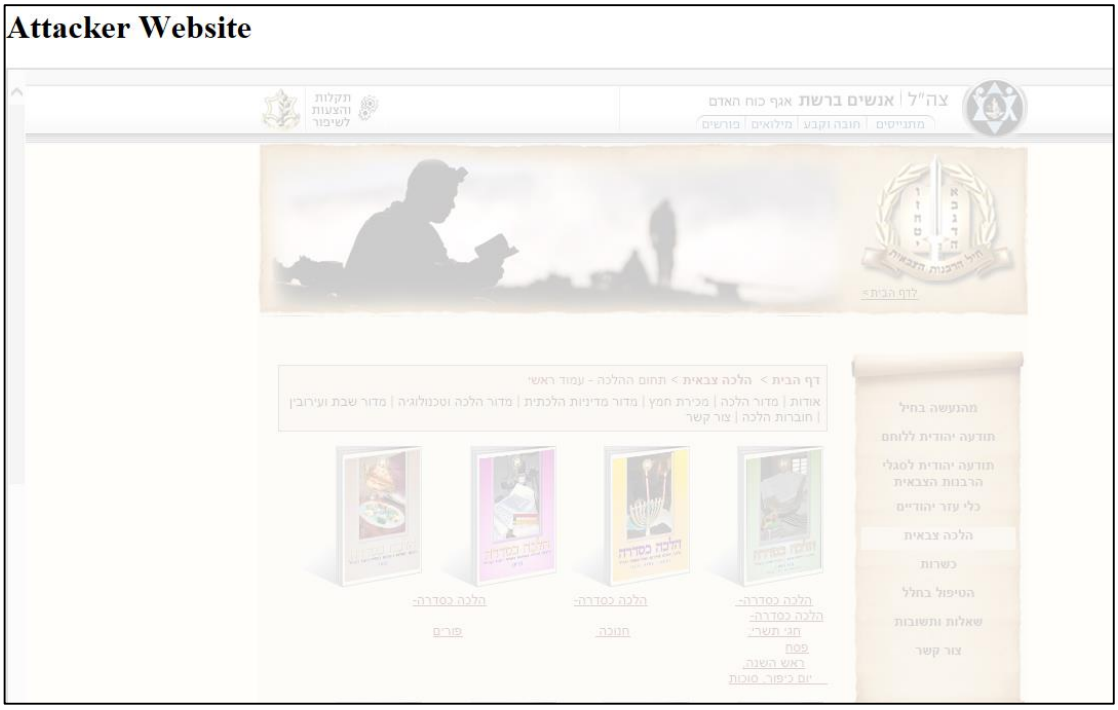
***פרטים טכניים***

כאשר גולשים לאתר הרבנות 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 הרבנות באתר מרוחק ולבצע הונאות שונות למשתמשי האתר באתרים זדוניים.

***הוכחת קיום ממצא:***

***דוגמא 1: הצגת תכנים של אתר הרבנות באתר מרוחק***



***<u>המלצות לתיקון</u>***

- 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