

מבדק חדירות

אתר חיל החינוך



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.....	לא קיימת הגנה מפני התקפת Clickjacking	.4.1
9.....	שירותים לא מוקשחים חושפים מידע פנימי אודות המערכת	.4.2

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	08.07.2015	אודי ברוך	דוח ראשון

הפצה

מ. גרסה	נמענים

2. כללי

2.1. הקדמה

מסמך זה מתאר את ממצאי בדיקת החדירות שבוצעה על מערכת חיל החינוך 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 חיל החינוך הינה מערכת המספקת מידע על החייל כמו תפקידים קיימים, תהליכי מיון ותוכניות ייחודיות.

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.

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'
נמוכה	Clickjacking	4.1
נמוכה	שירותים לא מוקשחים חושפים מידע פנימי אודות המערכת	4.2

4.1. 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 – Clickjacking היות וניתן להציג תכנים של אתר חיל החינוך באתרים מרוחקים ללא כל חסימה מצד הדפדפן. יש לציין כי הגדרות למניעת התקפות מסוג זה מגיעות מהשרת והחסימה בפועל מבוצעת בדפדפן שבצד הלקוח.

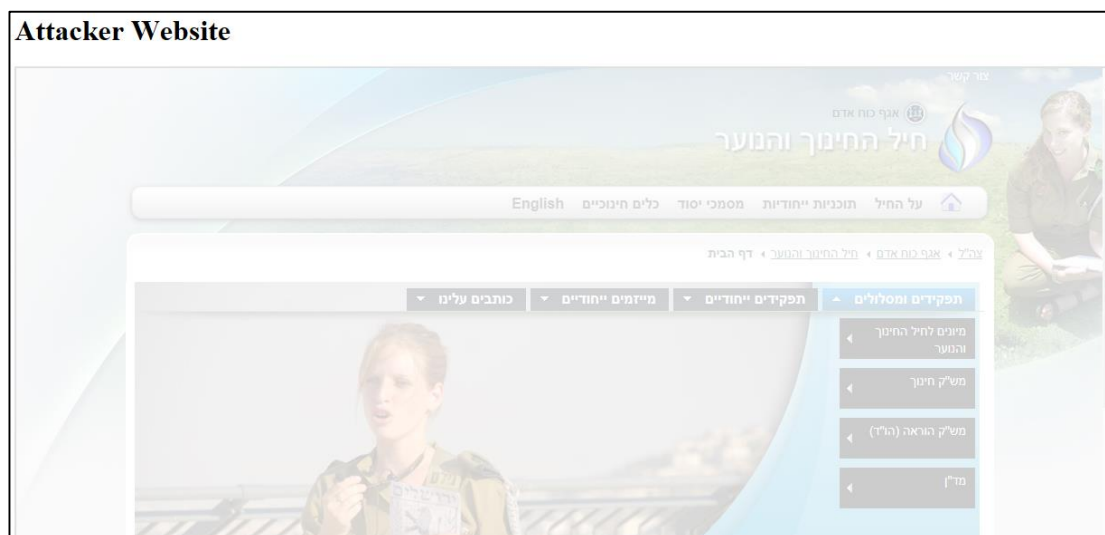
פרטים טכניים

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

הוכחת קיום ממצא:

דוגמא 1: הצגת תכנים של אתר חיל החינוך באתר מרוחק



המלצות לתיקון

- 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:

DENY – חסימה לגמרי –

SAMEORIGIN – מאופשר לאותו דומיין –

ALLOW-FROM - מאופשר לכתובת ספציפית -

4.2. 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

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 63799
Content-Type: text/html; charset=utf-8
Expires: -1
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Date: Wed, 08 Jul 2015 06:50:52 GMT
```

המלצות לתיקון

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