מבדק חדירות

אתר חיל הקשר והתקשוב

צוות אבטחת מידע

יולי, 2015

תוכן עניינים

1. מאפייני מסמך

מחבר	יוגב מזרחי
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	יוגב מזרחי	דוח ראשון

הפצה

מ. גרסה	נמענים

2. כללי

2.1 הקדמה

מסמך זה מתאר את ממצאי בדיקת החדירות שבוצעה על אתר חיל התקשוב במהלך חודש יולי 2015, שארכו כ שלושה ימים.

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

2.2 תיאור המערכת

אתר חיל התקשוב הינו אתר מקיף אודות חיל הקשר והתקשוב המציג חדשות ואירועים על החיל. האתר מכיל דפי מידע אודות היחידות השונות, תפקידים בחיל, גלריית וידאו ותמונות, פורומים המאפשרים לשאול שאלות ולהתייעץ. באתר קיים עמוד ליצירת קשר המאפשר למשתמשי האתר לפנות למוקד הפניות.

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 או מנהלי המערכת.
2. גורם כלשהו מצליח לחשוף מידע חיוני על המערכת.
3. גורם כלשהו עשוי לנצל פרצות אבטחה באתר עקב יישום ופיתוח לא מאובטח.

חשיפת המערכת לרשת האינטרנט במצבה הנוכחי עלולה להוות סיכון לפגיעה בתהליכים העסקיים של המערכת, במשתמשי המערכת ובמערכות המחשוב המקושרות אליה.

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	לא קיימת הגנה מפני פרסום אוטומטי בשירותי הפורומים	***גבוהה***
Error! Reference source not found.Error! Reference source not 4.2found.	מנגנון החיפוש באתר חושף את משתמשיו להתקפות מסוג הנדסה חברתית	**בינונית**
Error! Reference source not 4.3found.	שימוש ברכיבים לא מעודכנים	**בינונית**
Error! Reference source not found.Error! Reference source not found.Error! Reference source not 4.4found.	מנגנון ה- View State בשרת אינו מוצפן	***נמוכה***
Error! Reference source not 4.5found.	לא קיימת הגנה מפני התקפות "חטיפת קליקים" (Clickjacking)	***נמוכה***
4.6	שירותים לא מוקשחים חושפים מידע פנימי אודות המערכת	***נמוכה***

4.1 לא קיימת הגנה מפני פרסום אוטומטי בשירותי הפורומים

רמת חומרה: ***גבוהה***

סיווג ממצא: Denial of service

תיאור הבעיה

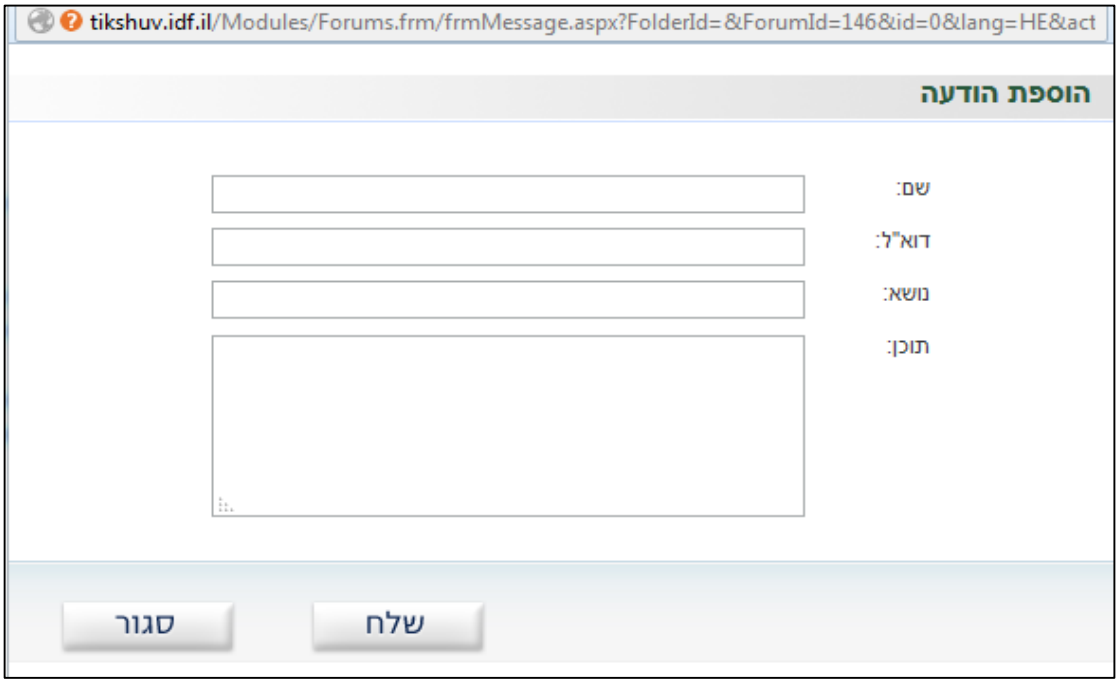
משתמשים זדוניים עלולים לגרום למניעת שירות באמצעות שליחת בקשות רבות בצורה אוטומטית למערכת הפורומים (לדוגמה הוספת פוסט חדש) ובכך לגרום להצפת מערכת הפורומים בתוכן סתמי ו\או פוגעני אשר יגרום לתוכן הרלוונטי הקיים באתר לא להופיע בעמודים הראשונים ובכך יפגע בחווית המשתמש. מעבר לכך הפצת תוכן רב בצורה אוטומטית עלולה להגדיל את נפח אחסון המידע באתר ובמקרי קיצון לגרום למניעת שירות עקב חוסר במקום פנוי.

פרטים טכניים

המערכת מאפשרת למשתמשיה להיכנס לפורומים השונים ולפרסם פוסטים חדשים או לחלופין לפרסם תגובות לפוסטים קודמים. בעת פרסום פוסט או תגובה, המערכת אינה בודקת כי שולח הבקשה אכן גורם אנושי ולא מערכת אוטומטית, מה שמאפשר למשתמשים זדוניים לייצר תהליך אוטומטי (לדוגמה באמצעות סקריפט שייכתבו) שבו יתפרסמו פוסטים ותגובות בלי הפסקה. התקפות אלה עלולות לפגוע במשאבי המערכת עד כדי מניעת שירות ו\או פגיעה בפונקציונאליות של המערכת ומשתמשיה.

הוכחת קיום ממצא:

דוגמה למסך הוספת הודעה במערכת אשר אינו מצריך captcha בעת ביצוע הפעולה



<u>המלצות לתיקון</u>

יש ליישם מנגנון אשר ימנע שימוש אוטומטי ולא אנושי במערכת. המלצה למנגנון העוזר בהגנה מפני כלים אוטומטיים הינו captcha. באמצעות הטמעת captcha במערכת הפורומים ניתן להקטין משמעותית את הסיכון לפגיעה בזמינות המערכת ומניעת פרסום תוכן לא רלוונטי בתדירות גבוהה. מעבר ליישום ה- captcha, מומלץ להטמיע במערכת מנגנון סינון תכנים אשר יבדוק את התוכן המוזן לפני פרסומו ובמקרה של תוכן זדוני, לא רלוונטי ו\או פוגעני, התוכן ייחסם ולא יפורסם.

4.2. מנגנון החיפוש באתר חושף את משתמשיו להתקפות מסוג הנדסה חברתית

רמת חומרה: ***בינונית***

סיווג ממצא: Input validation

תיאור הבעיה

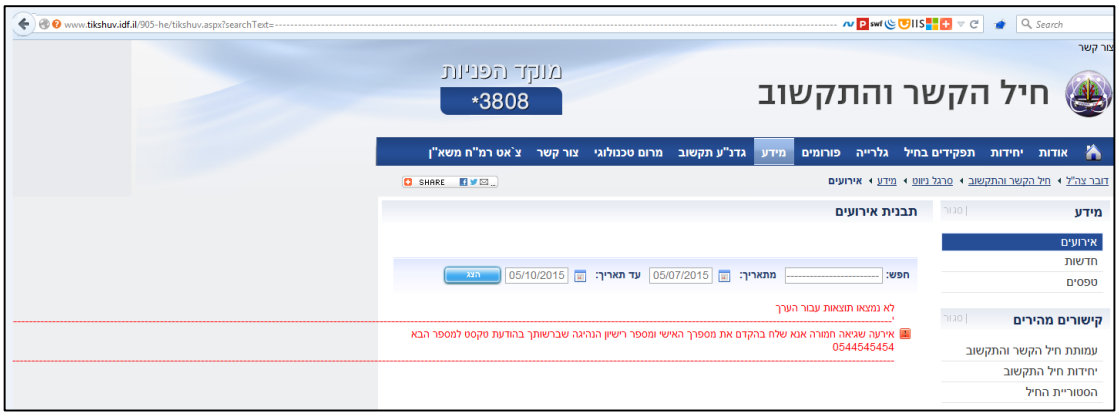
מנגנון החיפוש באתר מאפשר לגורמים זדוניים להזין קלט ארוך מהרגיל ובכך להציג את אותו קלט חזרה למשתמש. דבר זה עלול לגרום לפגיעה תדמיתית באתר ו\או להונאות משתמשי האתר באמצעות התקפות מסוג הנדסה חברתית. חשוב לציין כי היות והתוכן מוצג תחת כתובת URL לגיטימית של האתר, הסיכוי לפגיעה במשתמשי המערכת גבוה.

פרטים טכניים

מנגנון החיפוש באתר בנוי מכך שהמשתמש מזין את התוכן ברצונו לחפש ובמידה ותוכן זה אינו נמצא, האתר מודיע על כך שלא היו תוצאות לאותו חיפוש לצד הקלט שהוזן. החיפוש במערכת עובד בצורה כזו שנוצרת כתובת URL עם הפרמטר לחיפוש. היות ומנגנון החיפוש מאפשר להזין קלט ארוך מהרגיל, גורמים זדוניים עלולים לנצל זאת על ידי הכנסת תוכן זדוני לחיפוש ובכך לייצר קישור לגיטימי של האתר ובו התוכן הזדוני שהוזן ושליחתו למשתמשי ו\או מנהלי המערכת.

הוכחת קיום ממצא:

דוגמה לכתובת URL עם תוכן זדוני



המלצות לתיקון

- מומלץ לא להציג חזרה למשתמש את הקלט שהזין שלא לצורך.
- יש להגביל את אורך הקלט לחיפוש בהתאם למה שנדרש ובכל מקרה לא באורך של יותר ממשפט המכיל 2 מילים מה שכבר לא יהיה גם ככה רלוונטי לחיפוש.

- מומלץ לבצע בדיקת קלט על פי רשימה מותרת מראש (Whitelist) ובהתאם למה שנדרש בפועל במנגנון החיפש, לדוגמה אם אין צורך בחיפוש ספרות ו\או סימנים מסויימים כדוגמת "-" אז אין צורך כי תהיה למשתמש יכולת להזינם בחיפוש.

4.3 שימוש ברכיבים לא מעודכנים

רמת חומרה: ***בינונית***

סיווג ממצא: Implementation

תיאור הבעיה

במהלך המבדק נמצא כי האתר משתמש ברכיב jQuery בגרסה שאינה עדכנית ושקיימות בה בעיות אבטחה. שימוש בספריית jQuery לא מעודכנת חושף את האתר ומשתמשיו לבעיות אבטחה אשר התגלו באותה גרסה מה שעשוי לעזור לגורם זדוני לנצל זאת לצורך התקפות על משתמשי האתר.

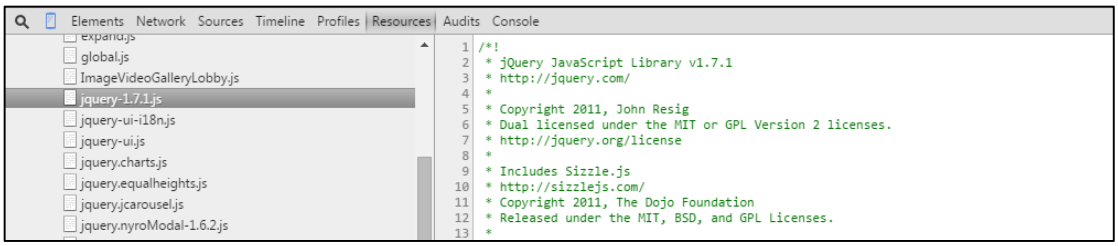
פרטים טכניים

כחלק מבדיקות המערכת נמצא כי נעשה שימוש באתר בספריית jQuery בגרסה ישנה, הגרסה בה נעשה שימוש הינה 1.7.2. גרסה זו חשופה לבעיית אבטחה מסוג XSS הנקראת "class selector XSS". בקישור הבא ניתן לראות את רשימת הגרסאות הפגיעות לחולשה זו לרבות גרסה 1.7.2 הקיימת באתר:

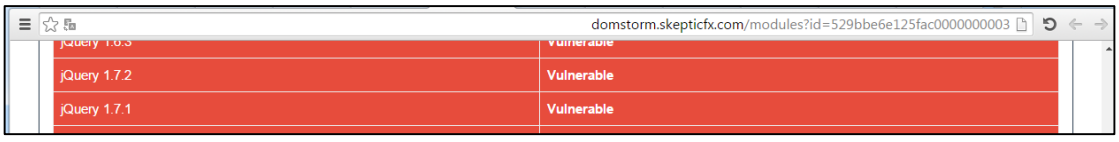
http://domstorm.skepticfx.com/modules?id=529bbe6e125fac0000000003

הוכחת קיום ממצא:

דוגמא 1: קיום ספריית jQuery לא עדכנית



דוגמא 2: זיהוי גרסה 1.7.2 כפגיעה



המלצות לתיקון

יש לבחון שדרוג של כל המודולים והתוספים באתר לגרסאות האחרונות בכדי להוריד את הסיכון לפגיעה במערכת. יש לעדכן לגרסה הכי עדכנית שניתן.

4.4 מנגנון ה- View State בשרת אינו מוצפן

רמת חומרה: ***נמוכה***

סיווג ממצא: Data Exposure

תיאור הבעיה

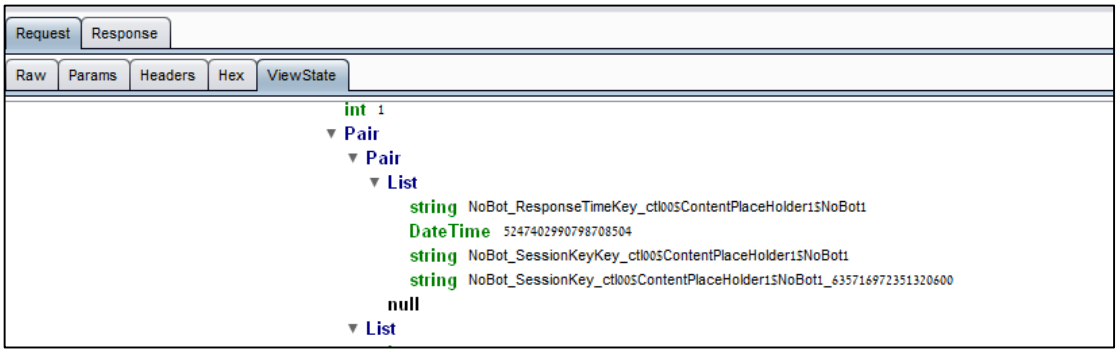
במהלך המבדק נבחנו הבקשות והתשובות השונות המועברות וחוזרות משרת המערכת ונמצא כי קיימת עבודה עם מנגנון ה- View State המכיל מידע בהתאם לבקשות השונות באתר. View State הינו מנגנון המאפשר לשמור נתונים בין הבקשות החוזרות והשונות באתר. לאחר ניתוח התעבורה נראה כי המידע המועבר בשרת במנגנון ה- View State הינו מקודד בלבד ולא מוצפן, מה שמאפשר לחשוף יותר מידע על אופי העבודה של המערכת בין הבקשות השונות באתר.

פרטים טכניים

כברירת מחדל באמצעות מנגנון ה- View State ניתן להעביר מידע בצורה שאינה מוצפנת אלא המידע מקודד בקידוד מסוג base64 אשר ניתן להמירו לטקסט רגיל ללא צורך בפיענוח הצפנה, עם זאת ניתן להגדיר כי המידע המועבר ב- View State יועבר תמיד בצורה מוצפנת מה שיחשוף פחות מידע אודות מבנה המערכת לגורם זדוני. לאחר בדיקת המידע המועבר במנגנון זה באתר, ניתן להבין כי המידע מקודד בלבד ואינו מוצפן ולכן ניתן להמירו לטקסט ולצפות בו.

הוכחת קיום ממצא:

זיהוי מידע במנגנון ה- View State



המלצות לתיקון

יש להגדיר בהגדרות הדף את הצפנת ה- View State באמצעות ההגדרה הבאה:

ViewStateEncryptionMode="Always"

ובכך המידע המועבר שם יועבר תמיד בצורה מוצפנת.

4.5 לא קיימת הגנה מפני התקפות "חטיפת קליקים" (Clickjacking)

רמת חומרה: ***בינונית***

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 (לדוגמה במאמצעות iframe) מה שחושף את משתמשי האתר להתקפות מסוג Phishing ו – Clickjacking היות וניתן להציג תכנים של אתר חיל התקשוב 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

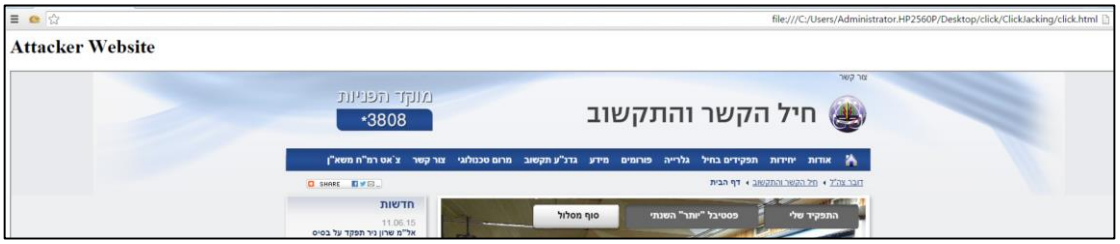
כאשר גולשים לאתר חיל התקשוב מתקבלות כותרות מצד השרת אל הדפדפן של הגולש ולפיהן הדפדפן מבצע פעולות שונות בצד הלקוח. להלן הכותרות המתקבלות בעת גלישה לאתר:

```
HTTP/1.1 302 Found
Cache-Control: private
Content-Length: 727
Content-Type: text/html; charset=utf-8
Location: /894-he/tikshuv.aspx
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Date: Tue, 07 Jul 2015 06:03:25 GMT
```

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 התקשוב באתר מרוחק ולבצע הונאות שונות למשתמשי האתר באתרים זדוניים.

<u>הוכחת קיום ממצא:</u>

הצגת תכנים של אתר חיל התקשוב 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:
  - DENY – חסימה לכולם
  - SAMEORIGIN – מאפשר לאותו דומיין
  - ALLOW-FROM - מאפשר לכתובת ספציפית
- להלן דוגמה להגדרה בקובץ ה- web.config להצגת תוכן באותו דומיין בלבד:

```
<system.webServer>
  <httpProtocol>
    <customHeaders>
      <add name="X-Frame-Options" value="SAMEORIGIN" />
    </customHeaders>
  </httpProtocol>
</system.webServer>
```

במידה ואין צורך להצגה מרוחקת של התכנים, יש להגדיר את ה- *Value* על ערך ה- *Deny*.

4.6 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 כי המערכת עובדת על גבי פלטפורמת ASP.NET, ובנוסף נחשפת הגרסה המדוייקת המתוקנת בשרת, מספר הגרסה שנחשף הינו *4.0.30319*.

הוכחת קיום ממצא:

זיהוי גרסת ה-ASP.NET

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 49660
Content-Type: text/html; charset=utf-8
Expires: -1
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Date: Sun, 05 Jul 2015 12:48:31 GMT


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

המלצות לתיקון

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