מבדק חדירות

אתר חיל הרפואה

צוות אבטחת מידע

מאי, 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	31.05.2015	יוגב מזרחי	דוח ראשון

הפצה

מ. גרסה	נמענים

2. כללי

2.1 הקדמה

מסמך זה מתאר את ממצאי בדיקת החדירות שבוצעה על אתר חיל הרפואה 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 חיל הרפואה מספק לגולשים שירות מקוון ורחב אודות חיל הרפואה, שירותי הרפואה השונים הקיימים בצה"ל, חדשות ואירועים, גלרית תמונות, כתבות ועוד. האתר מספק מגוון קישורים נוספים לאתרי צהל השונים. באתר קיים טופס ליצירת קשר.

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 ,מהווה 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
Error! Reference source not found. 4.1	Host header poisoning	***קריטית***
Error! Reference source not found. 4.2	קבצי האתר חושפים מידע רגיש על הארגון	**בינונית**
Error! Reference source not found. 4.3	שימוש ברכיבים לא מעודכנים	**בינונית**
4.4.4	לא קיימת הגנה מפני התקפות "חטיפת קליקים" (Clickjacking)	**בינונית**
4.5.4	מנגנון ה- View State בשרת אינו מוצפן	***נמוכה***
4.6	שרתים לא מוקשחים חושפים מידע פנימי אודות המערכת	***נמוכה***

4.1 Host header poisoning

רמת חומרה: ***קריטית***

סיווג ממצא: *Input and Data Validation*

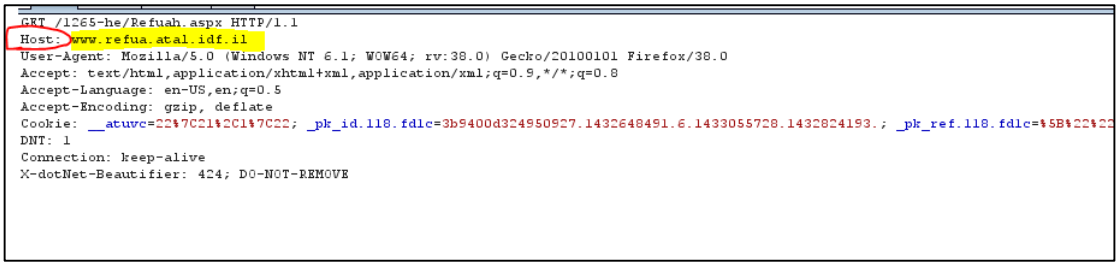
תיאור הבעיה

במהלך המבדק נמצא כי קישורים הקיימים בעמודי האתר נוצרים בצורה דינאמית על בסיס כותרת השרת הנקראת "Host Header". כותרת ה- host header מציינת את כתובת השרת בו האתר מאוחסן והיא מופיעה בכל בקשה הנשלחת מהמשתמש לשרת, עקב כך כי לא מתבצעת בדיקה על התוכן המוזן בכותרת, ברשות המשתמש האפשרות לשנות את הכתובת לכתובת של אתר זדוני. היות וקישורים באתר מורכבים מהמידע המוזן בכותרת זו, משתמש זדוני יכול לשנות את הכותרת ולגרום לשינוי התוכן הדינאמי המוצג באתר בצד הלקוח, הדרכים העיקריות לניצול חשיפה זו:

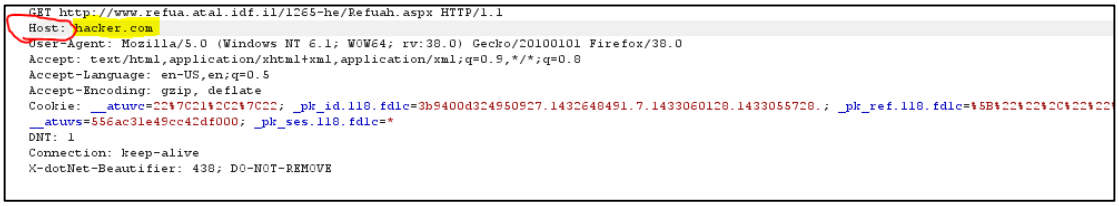
- יצירת עמוד פיקטיבי המפנה לאתר חיל הרפואה האמיתי וגורם לשינוי הקישורים באתר, בשיטה זו ברגע שמשתמש יבקר באתר חיל הרפואה דרך העמוד הפיקטיבי, תהיה לתוקף אפשרות לשלוט בקישורים אשר יוצגו באתר, יש לציין כי המשתמש בסופו של דבר יבקר באתר האמיתי של חיל הרפואה ולא באתר מזוייף ולכן לא יהיה לו במה לחשוש (יש לציין כי מימוש החשיפה באמצעות שיטה זו קיים באתר)..
- במידה והאתר משתמש בשירותי cache השומרים זמנית תכנים באתר לצורך שיפור הטעינה, ייתכן כי בעת שינוי הקישורים באתר בצד המשתמש, תהיה השפעה רוחבית על משתמשים אחרים היות והתוכן ישמר ב- cache בשרת\ים.
- שליחת קישור דרך האתר המסתמך על כותרת ה- host header לדוגמה: איפוס סיסמה או שלח לחבר (יש לציין כי מימוש החשיפה באמצעות שיטה זו קיים באתר באמצעות אפשרות "שלח לחבר").

פרטים טכניים

כותרת ה- host header, מייצגת את כתובת השרת בו האתר מאוחסן. ברגע שגולש מבצע פנייה לאתר כחלק מהבקשה הוא מציין את כתובת ה- host אליה הוא פונה בנוסף לכתובת המלאה של העמוד הספציפי אליו הוא גולש, להלן דוגמה לבקשה לגיטימית באתר:



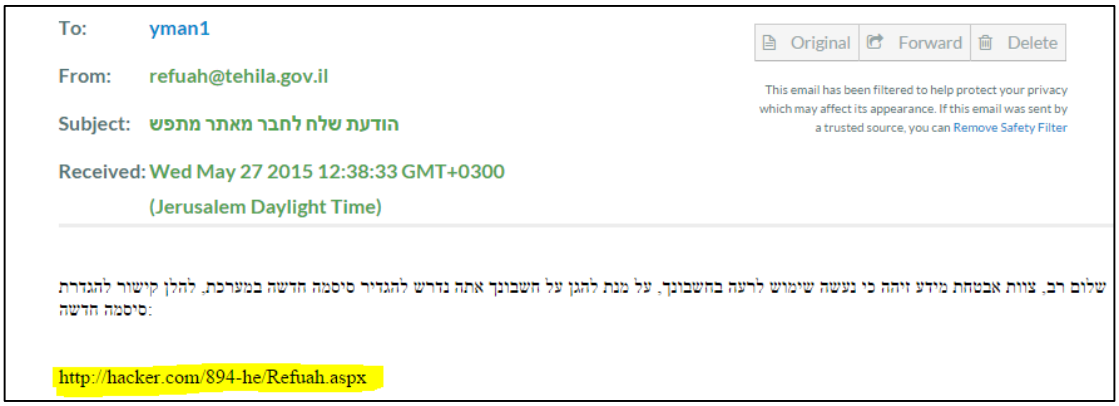
להלן דוגמה לבקשה לאותו עמוד עם שינוי כותרת ה- host:



<u>הוכחת קיום ממצא:</u>

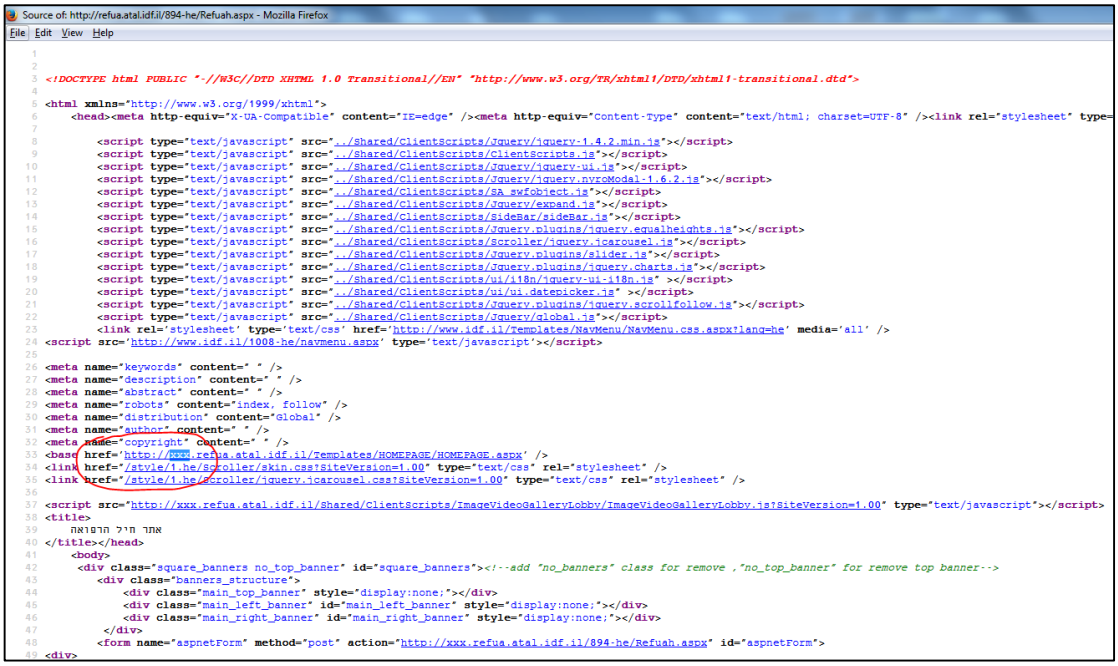
דוגמא 1: שינוי קישור הנשלח במייל באמצעות שלח לחבר

בעת שינוי כתובת ה- host header ניתן לשלוט בקישור אשר יישלח במייל למשתמשים באמצעות שלח לחבר:



דוגמא 2: שינוי קישורים באתר

בעת שינוי כתובת ה- host header ניתן לראות כי הקישורים באתר שונו:




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

<html xmlns="http://www.w3.org/1999/xhtml">
    <head><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><link rel="stylesheet" type=

        <script type="text/javascript" src="../Shared/ClientScripts/Jquery/jquery-1.4.2.min.js"></script>
        <script type="text/javascript" src="../Shared/ClientScripts/ClientScripts.js"></script>
        <script type="text/javascript" src="../Shared/ClientScripts/Jquery/jquery-ui.js"></script>
        <script type="text/javascript" src="../Shared/ClientScripts/Jquery/jquery.nyroModal-1.6.2.js"></script>
        <script type="text/javascript" src="../Shared/ClientScripts/SA_swfObject.js"></script>
        <script type="text/javascript" src="../Shared/ClientScripts/Jquery/expand.js"></script>
        <script type="text/javascript" src="../Shared/ClientScripts/SideBar/sideBar.js"></script>
        <script type="text/javascript" src="../Shared/ClientScripts/Jquery.plugins/jquery.equalheights.js"></script>
        <script type="text/javascript" src="../Shared/ClientScripts/Scroller/jquery.icarousel.js"></script>
        <script type="text/javascript" src="../Shared/ClientScripts/Jquery.plugins/slider.js"></script>
        <script type="text/javascript" src="../Shared/ClientScripts/Jquery.plugins/jquery.charts.js"></script>
        <script type="text/javascript" src="../Shared/ClientScripts/ui/i18n/jquery-ui-i18n.js" ></script>
        <script type="text/javascript" src="../Shared/ClientScripts/ui/ui.datepicker.js" ></script>
        <script type="text/javascript" src="../Shared/ClientScripts/Jquery.plugins/jquery.scrollfollow.js"></script>
        <script type="text/javascript" src="../Shared/ClientScripts/Jquery/global.js"></script>
        <link rel='stylesheet' type='text/css' href='http://www.idf.il/Templates/NavMenu/NavMenu.css.aspx?lang=he' media='all' />
<script src='http://www.idf.il/1008-he/navmenu.aspx' type='text/javascript'></script>

<meta name="keywords" content=" " />
<meta name="description" content=" " />
<meta name="abstract" content=" " />
<meta name="robots" content="index, follow" />
<meta name="distribution" content="Global" />
<meta name="author" content=" " />
<meta name="copyright" content=" " />
<base href='http://xxx.refua.atal.idf.il/Templates/HOMEPAGE/HOMEPAGE.aspx' />
<link href="/style/1.he/Scroller/skin.css?SiteVersion=1.00" type="text/css" rel="stylesheet" />
<link href="/style/1.he/Scroller/jquery.icarousel.css?SiteVersion=1.00" type="text/css" rel="stylesheet" />

<script src="http://xxx.refua.atal.idf.il/Shared/ClientScripts/ImageVideoGalleryLobby/ImageVideoGalleryLobby.js?SiteVersion=1.00" type="text/javascript"></script>
<title>
    אתר חיל הרפואה
</title></head>
    <body>
     <div class="square_banners no_top_banner" id="square_banners"><!--add "no_banners" class for remove ,"no_top_banner" for remove top banner-->
        <div class="banners_structure">
            <div class="main_top_banner" style="display:none;"></div>
            <div class="main_left_banner" id="main_left_banner" style="display:none;"></div>
            <div class="main_right_banner" id="main_right_banner" style="display:none;"></div>
         </div>
        <form name="aspnetForm" method="post" action="http://xxx.refua.atal.idf.il/894-he/Refuah.aspx" id="aspnetForm">
<div>
```

<u>המלצות לתיקון</u>

- שימוש בתוכן דינאמי המורכב מכותרת ה- host header בדרך כלל מיושם במקרים בהם אותו שרת מאחסן מספר אתרים שונים, ולכן יש לבחון אם אכן יש צורך ביישום זה במצב הנוכחי, במידה ולא, יש לשנות את הקישורים באתר או כל תוכן דינאמי אחר המסתמך על מידע המתקבל מכותרת זו לתוכן סטטי או לחלופין לתוכן דינאמי המתבסס על מידע מצד השרת בלבד.במידה ובכל זאת יש צורך לשימוש בתצורה זו, יש לבצע בדיקות קלט על התוכן המוזן בכותרת המגיעה מצד המשתמש ובנוסף לאמת את הכתובות מול רשימת כתובות המותרות מראש (whitelist) כך שלא יתאפשר להכניס כתובת של אתר זדוני.

4.2 <u>קבצי האתר חושפים מידע רגיש על הארגון</u>

רמת חומרה: ***בינונית***

סיווג ממצא: *Data Exposure*

<u>תיאור הבעיה</u>

במהלך המבדק בוצע תהליך איסוף מידע אודות האתר והקבצים הפומביים המאוחסים בו, לאחר חילוץ המידע וניתוחו נמצא מידע רב הרגיש לארגון, מידע זה עשוי להיות חיוני מאוד לגורם זדוני בעת ביצוע התקפות מכוונות על הארגון.

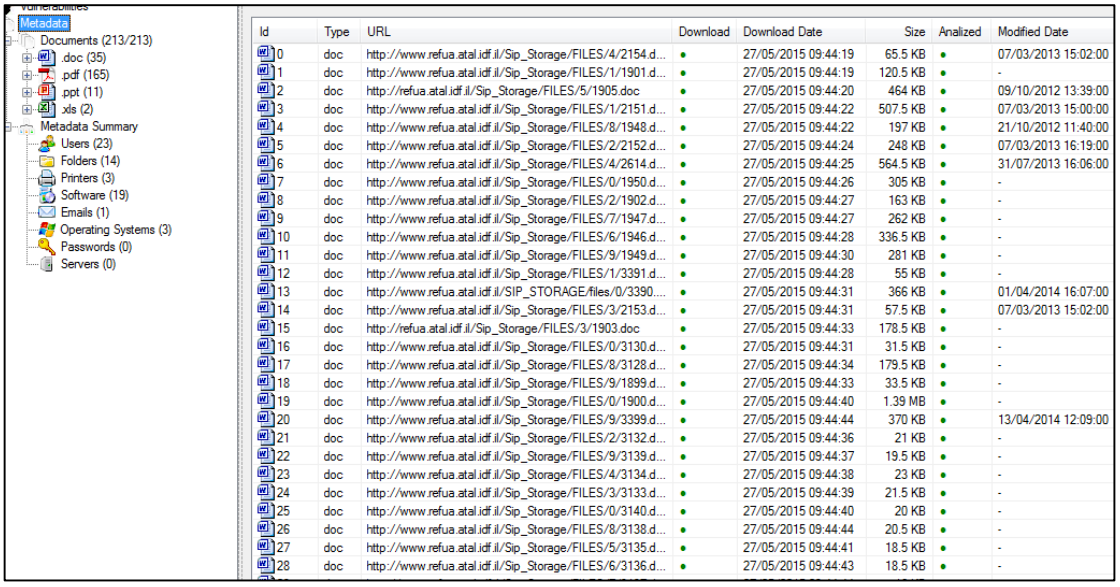
<u>פרטים טכניים</u>

במהלך המבדק ביצענו סריקה לאיתור קבצים פומביים הקיימים באתר כגון קבצי WORD, קבצי PDF, קבצי EXCEL ועוד. לאחר הורדת הקבצים למחשב הבדיקה, ביצענו ניתוח למאפייני ה- Meta Data של הקבצים וחילצנו את המידע המצוי בהם. להלן פרטי הנתונים אותם הצלחנו לחלץ מהקבצים:

- 23 שמות משתמשים אשר כתבו\יצרו את המסמכים.
- 2 נתיבים פנימיים לקבצים ותיקיות במחשבים בהם יצרו את המסמכים.
- 3 סוגי מערכות הפעלה בהן נוצרו הקבצים.
- 3 מדפסות פנימיות בארגון.
- 19 תוכנות פנימיות המשמשות את מחשבי הארגון.

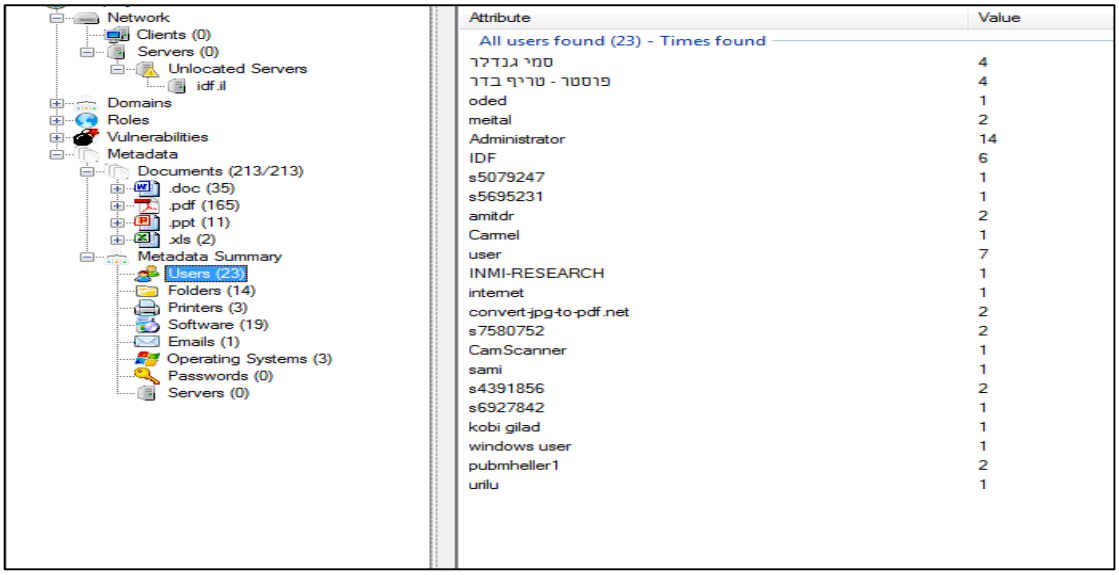
<u>הוכחת קיום ממצא:</u>

דוגמא 1: חלק מהקבצים אשר הורדו למחשב



Id	Type	URL	Download	Download Date	Size	Analized	Modified Date
0	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/4/2154.d...	•	27/05/2015 09:44:19	65.5 KB	•	07/03/2013 15:02:00
1	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/1/1901.d...	•	27/05/2015 09:44:19	120.5 KB	•	-
2	doc	http://refua.atal.idf.il/Sip_Storage/FILES/5/1905.doc	•	27/05/2015 09:44:20	464 KB	•	09/10/2012 13:39:00
3	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/1/2151.d...	•	27/05/2015 09:44:22	507.5 KB	•	07/03/2013 15:00:00
4	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/8/1948.d...	•	27/05/2015 09:44:22	197 KB	•	21/10/2012 11:40:00
5	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/2/2152.d...	•	27/05/2015 09:44:24	248 KB	•	07/03/2013 16:19:00
6	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/4/2614.d...	•	27/05/2015 09:44:25	564.5 KB	•	31/07/2013 16:06:00
7	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/0/1950.d...	•	27/05/2015 09:44:26	305 KB	•	-
8	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/2/1902.d...	•	27/05/2015 09:44:27	163 KB	•	-
9	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/7/1947.d...	•	27/05/2015 09:44:27	262 KB	•	-
10	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/6/1946.d...	•	27/05/2015 09:44:28	336.5 KB	•	-
11	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/9/1949.d...	•	27/05/2015 09:44:30	281 KB	•	-
12	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/1/3391.d...	•	27/05/2015 09:44:28	55 KB	•	-
13	doc	http://www.refua.atal.idf.il/SIP_STORAGE/files/0/3390....	•	27/05/2015 09:44:31	366 KB	•	01/04/2014 16:07:00
14	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/3/2153.d...	•	27/05/2015 09:44:31	57.5 KB	•	07/03/2013 15:02:00
15	doc	http://refua.atal.idf.il/Sip_Storage/FILES/3/1903.doc	•	27/05/2015 09:44:33	178.5 KB	•	-
16	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/0/3130.d...	•	27/05/2015 09:44:31	31.5 KB	•	-
17	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/8/3128.d...	•	27/05/2015 09:44:34	179.5 KB	•	-
18	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/9/1899.d...	•	27/05/2015 09:44:33	33.5 KB	•	-
19	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/0/1900.d...	•	27/05/2015 09:44:40	1.39 MB	•	-
20	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/9/3399.d...	•	27/05/2015 09:44:44	370 KB	•	13/04/2014 12:09:00
21	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/2/3132.d...	•	27/05/2015 09:44:36	21 KB	•	-
22	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/9/3139.d...	•	27/05/2015 09:44:37	19.5 KB	•	-
23	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/4/3134.d...	•	27/05/2015 09:44:38	23 KB	•	-
24	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/3/3133.d...	•	27/05/2015 09:44:39	21.5 KB	•	-
25	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/0/3140.d...	•	27/05/2015 09:44:40	20 KB	•	-
26	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/8/3138.d...	•	27/05/2015 09:44:44	20.5 KB	•	-
27	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/5/3135.d...	•	27/05/2015 09:44:41	18.5 KB	•	-
28	doc	http://www.refua.atal.idf.il/Sip_Storage/FILES/6/3136.d...	•	27/05/2015 09:44:43	18.5 KB	•	-

דוגמא 2: דוגמה לשמות המשתמשים שחולצו



***ראה נספח א' המכיל את הפרטים המלאים של הנתונים שחולצו.**

<u>המלצות לתיקון</u>

- יש לבחון את המסמכים המפורסמים באתר ולמחוק את כל המידע הלא הכרחי המצוי במאפייני הקובץ (Meta Data).
- בכדי למנוע בעיה זו בעתיד, מומלץ להכניס להתהליך פרסום המסמכים באתר, שלב שבו יימחקו כל הנתונים לפני פרסומם.

4.3 <u>שימוש ברכיבים לא מעודכנים</u>

רמת חומרה: ***בינונית***

סיווג ממצא: *Configuration*

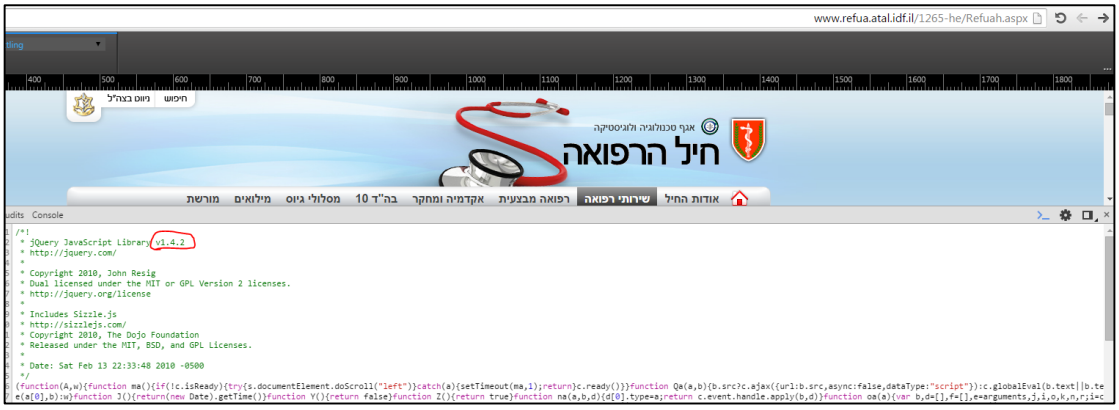
<u>תיאור הבעיה</u>

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 (גרסה 1.4.2). להלן קישור לפירצות אבטחה מסוג XSS (Cross Site Scripting) אשר התגלתה בגרסה הקיימת באתר:

http://seclists.org/fulldisclosure/2014/Sep/10

<u>פרטים טכניים</u>

כחלק מבדיקות המערכת נמצא כי נעשה שימוש באתר בספריית jQuery בגרסה ישנה, הגרסה בה נעשה שימוש הינה 1.4.2. להלן תמונה הממחישה את הרצת גרסה זו באתר:



היות וגרסה זו חשופה לבעיות אבטחה מסוג XSS, באפשרות גורם זדוני להכין עמוד פיקטיבי אשר גורם להרצה מרחוק של קובץ הג'אווה סקריפט של ספריית ה- jQuery היושב באתר בנתיב הבא:

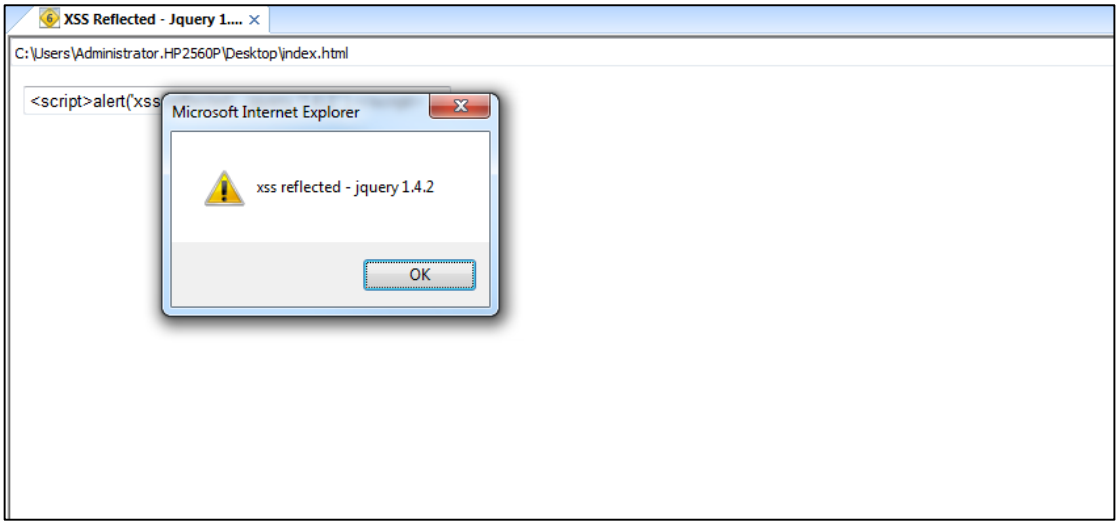
http://www.refua.atal.idf.il/Shared/ClientScripts/Jquery/jquery-1.4.2.min.js

ולהריץ קוד זדוני בצד הלקוח. דוגמה לעמוד פקטיבי הגורם להתקפת XSS באמצעות קובץ ה- jQuery של האתר:

```
<html>
<head>
  <meta charset="utf-8">
  <title>XSS Reflected - Jquery 1.4.2 </title>
  <script src="http://www.refua.atal.idf.il/Shared/ClientScripts/Jquery/jquery-1.4.2.min.js"></script>
  <script>
    $(function() {
      $('#users').each(function() {
        var select = $(this);
        var option = select.children('option').first();
        select.after(option.text());
        select.hide();
      });
    });
  </script>
</head>


<body>
  <form method="post">
    <p>
      <select id="users" name="users">
        <option value="xssreflected">&lt;script&gt;alert(&#x27;xss
reflected - jquery 1.4.2 &#x27;);&lt;/script&gt;</option>
      </select>
    </p>
  </form>
</body>
</html>
```

ובעת ביקור בעמוד זה אנו מקבלים הודעה הקופצת למשתמש:



<u>הוכחת קיום ממצא:</u>

דוגמא 1: קיום גרסה ישנה של jquey 1.4.2

<u>המלצות לתיקון</u>

- יש לבחון שדרוג של כל המודולים והתוספים באתר לגרסאות האחרונות בכדי להוריד את הסיכון לפגיעה במערכת. יש לוודא תחילה את תאימות האתר לגרסאות האחרונות ובמידה וקיימת גרסה שאינה תואמת לאתר, יש לעדכן לגרסה הכי עדכנית

שניתן. לגבי ספריית jQuery יש לבחון את תמיכת האתר בגרסה 2.x, במידה ונתמך יש לעדכן לגרסה 2.1.3, במידה ולא יש לעדכן לגרסה 1.11.2.

4.4. 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 (iframe) מה שחושף את משתמשי האתר להתקפות מסוג Phishing ו – Clickjacking היות וניתן להציג תכנים של אתר חיל הרפואה 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

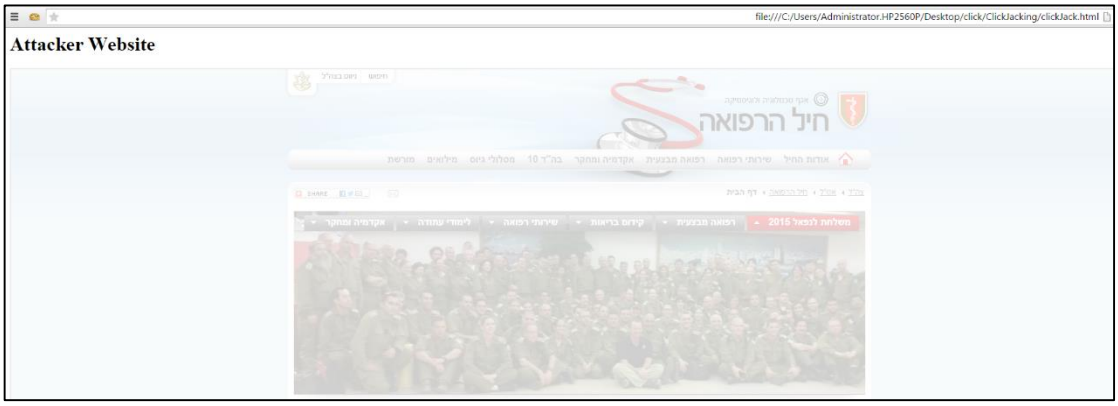
כאשר גולשים לאתר חיל הרפואה מתקבלות כותרות מצד השרת אל הדפדפן של הגולש ולפיהן הדפדפן מבצע פעולות שונות בצד הלקוח. כיום בעת גלישה לאתר, להלן הכותרות המתקבלות:

```
HTTP/1.1 200 OK
Date: Sun, 31 May 2015 14:22:04 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Cache-Control: no-cache
Pragma: no-cache
Expires: -1
Content-Type: text/html; charset=utf-8
Content-Length: 656508
```

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 החיל הרפואה באתר מרוחק ולבצע הונאות שונות למשתמשי האתר באתרים זדוניים.

<u>הוכחת קיום ממצא:</u>

דוגמא 1: הצגת תכנים של אתר חיל הרפואה 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 לגמרי
  - 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 להצגת מרוחקת של התכנים, יש להגדיר את ה- Value על ערך -v ה- Deny.

4.5. <u>מנגנון ה- View State בשרת אינו מוצפן</u>

רמת חומרה: נמוכה

סיווג ממצא: *Data Exposure*

<u>תיאור הבעיה</u>

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.

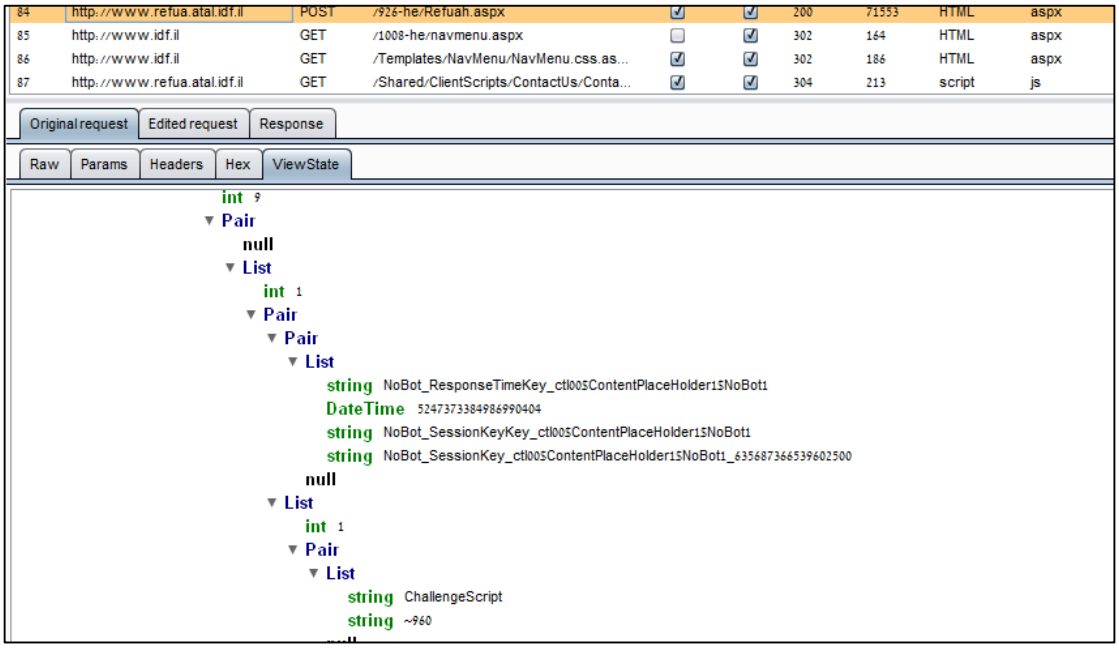
<u>פרטים טכניים</u>

בעת גלישה באתר ניתן להבחין כי קיימת עבודה עם מנגנון ה- View State. להלן תמונה המציגה את פרמטר ה- View State הקיים בבקשות השונות באתר:

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.

<u>הוכחת קיום ממצא:</u>

דוגמא 1: זיהוי מידע במנגנון ה- View State



<u>המלצות לתיקון</u>

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

```
ViewStateEncryptionMode="Always"
```

ובכך המידע המועבר שם יועבר תמיד בצורה מוצפנת.

4.6 <u>שרתים לא מוקשחים חושפים מידע פנימי אודות המערכת</u>

רמת חומרה: נמוכה

סיווג ממצא: *Configuration*

<u>תיאור הבעיה</u>

המערכת חושפת מידע אודות עצמה: גרסת IIS, פלטפורמת פיתוח, גרסת ASP .NET וכו'.

עובדה זו מאפשרת לתוקפים לאסוף מידע אודות המערכת ולבצע התקפה ממוקדת יותר.

```
HTTP/1.1 200 OK
Date: Mon, 01 Jun 2015 06:23:01 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Cache-Control: no-cache
Pragma: no-cache
Expires: -1
Content-Type: text/html; charset=utf-8
Content-Length: 656508



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

<html xmlns="http://www.w3.org/1999/xhtml">
    <head><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta http-equiv="Content-Type" cont
href="/Style/Shared/text.css" media="all" /><link rel="stylesheet" type="text/css" href="/Style/Share
href="/Style/Shared/layout2.css" media="all" /><link rel="stylesheet" type="text/css" href="/Style/Sh
href="/Style/Shared/datepicker.css" media="all" /><link rel="stylesheet" type="text/css" href="/Style
href="/Style/1.HE/print.css" media="print" /><!--[if IE 6]><link rel="stylesheet" type="text/css" hre
```

<u>פרטים טכניים</u>

- אין לחשוף מידע פנימי אודות המערכת והתשתיות שלה – יש לבצע הקשחה לשרתים השונים של המערכת.
  - בשרת ה IIS יש לחסום את האפשרות להציג את הגרסה של השרת ב-Response.
  - בשרת האפליקציה יש להקשיח את ההגדרות של ASP.NET.
- מומלץ לקרוא את המאמר הבא להבנה מעמיקה של הנושא:

https://www.owasp.org/index.php/Testing_for_Web_Application_Fingerprint_(OWASP-IG-004)

5. נספח א' - פירוט מידע מקבצי האתר

metadata-info.xlsx