בדיקת חוסן אפליקטיבית חוזרת – מערכת חימוש

עבור

ממשל זמין

בוצע ע"י:

יגאל אלפנט

יועץ אבטחת מידע

חברת 2Bsecure בע"מ

רח' הערבה 3, קריית שדה התעופה. טלפון:03-6492007 פקס: 03-6492008
דוא"ל: info@2bsecure.co.il. אתר: www.2bsecure.co.il

תוכן עניינים

לכבוד: מר. אברהם זרוק **תאריך:** **24/12/2014**

הנדון: בדיקת חוסן אפליקטיבית – מערכת חימוש

פרק א' – תקציר מנהלים

כללי

בחודש דצמבר 2014 זומנה חברת 2bsecure לבצע בדיקה אפליקטיבית חוזרת למערכת חימוש. הבדיקה המקורית בוצעה בחודש נובמבר 2014. הבדיקה התבצעה על המערכת בכתובת הבאה:

http://www.chimush.atal.idf.il

סיכום

בבדיקה נמצא כי חלק גדול ממצאי המערכת לא תוקנו באופן מספק.
כתוצאה, המערכת נמצאת בסיכון **גבוה** למתקפות אפליקטיביות. מומלץ לתקן את ממצאי הבדיקה ולבצע בדיקה חוזרת בטרם הפצת המערכת.

טבלת סטטוס ממצאים

לפניך טבלת סיכום הכוללת את סטטוס הממצאים.

מס	שם הממצא	חומרה	סטטוס	הסבר
.1	שימוש ברכיבי תוכנה פגיעים	**גבוהה**	**לא תוקן**	
.2	משתנה ViewState אינו מוצפן	**בינונית**	**לא תוקן**	במספר מקומות נמצא כי הוא מוצפן אך לא בכל המערכת.
.3	Debug פעיל בצד השרת	**בינונית**	**תוקן**	
.4	דליפת מידע דרך רכיבי Flash	**בינונית**	**לא תוקן**	נמצא כי תוקן לגבי חלק מרכיבי ה Flash אך לא לגבי כולם
.5	חשיפת גרסת השרת	**נמוכה**	**לא תוקן**	
.6	שימוש בשם ברירת מחדל של ה cookie	**נמוכה**	**תוקן**	

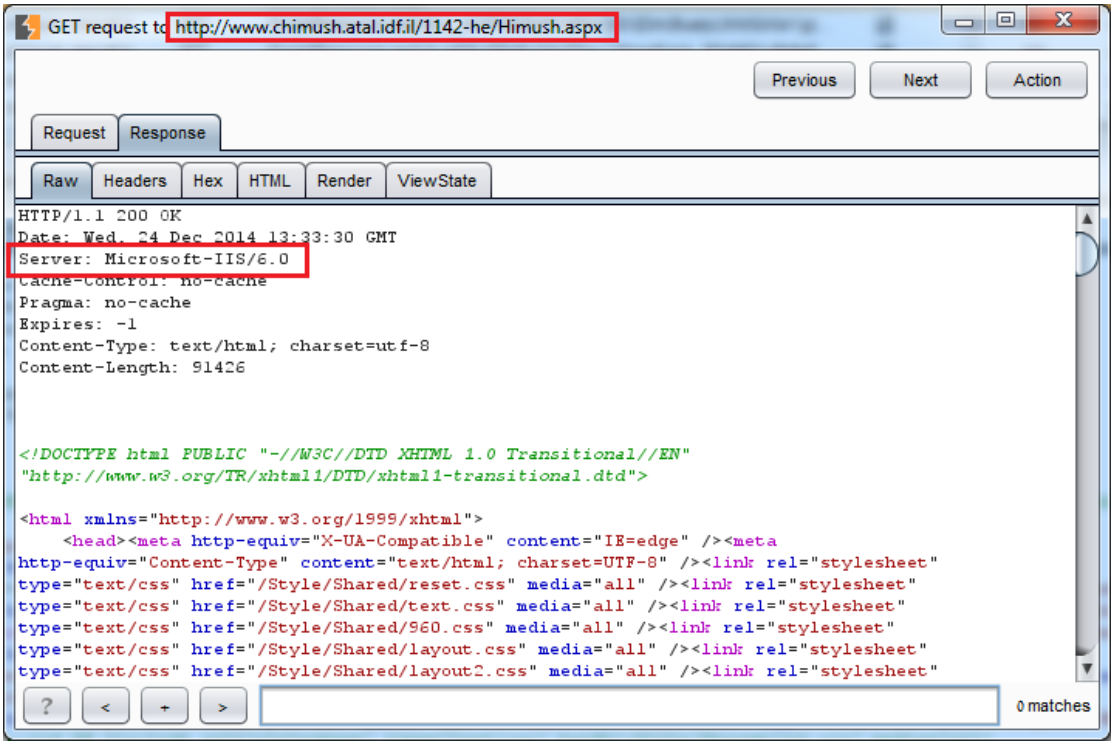
כמו כן, במהלך הבדיקה החוזרת נמצא במערכת ממצא נוסף:

פרק ב' – פרטי הממצאים שלא תוקנו

מספרי הממצאים בפרק זה תואמים את מספרי הממצאים במסמך המקורי ולכן ייתכן מאוד שהמספרים אינם רציפים.

1. שימוש ברכיבי תוכנה פגיעים

להלן צילום מסך מהבדיקה החוזרת:

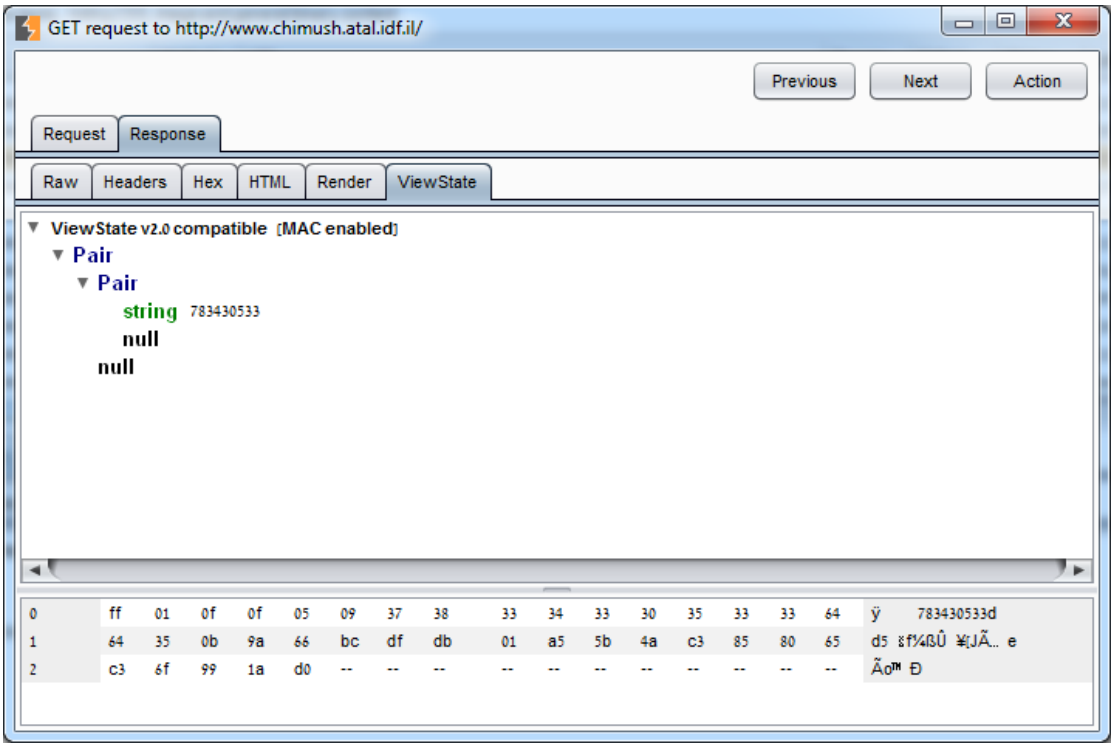


אמצעי נגד:

1. מומלץ לשדרג את גרסת השרת.

2. משתנה ViewState אינו מוצפן

להלן צילום מסך של משתנה ה ViewState כפי שנמצא במהלך הבדיקה החוזרת:



אמצעי נגד:

1. מומלץ להצפין את משתנה ה View State -באמצעות ההצהרה המובנת של .NET. בראש כל דף:

```
<%@Page ViewStateEncryptionMode="Always" %>
```

2. מומלץ להשתמש בפרמטר ViewStateUserKey כדי למנוע מתקפות.CSRF

למידע נוסף בנושא:

http://msdn.microsoft.com/en-us/library/system.web.ui.page.viewstateuserkey(v=vs.110).aspx

4. דליפת מידע דרך רכיבי Flash

להלן צילום מסך של הגדרות Flash כפי שנמצאו במערכת:

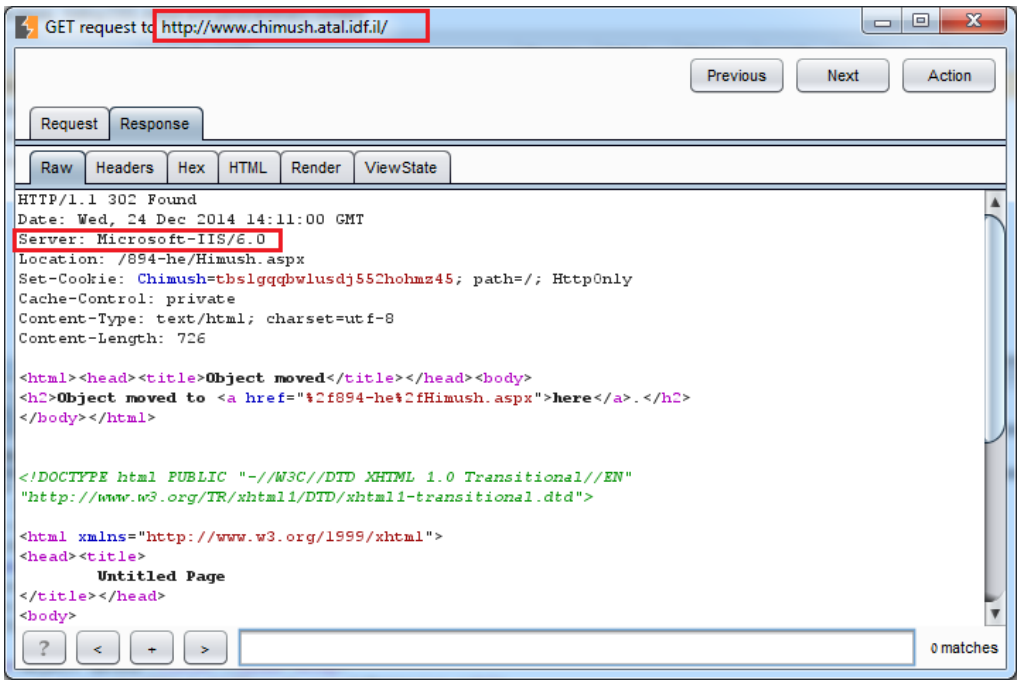
```
http://www.chi...entscripts.js
www.chimush.atal.idf.il/shared/clientscripts/clientscripts.js
    }

    $(".galleryWindow:eq(" + idx + ")").fadeOut("slow", function() {
        ClearVideoParams(idx);
        $(".videoWrapper:eq(" + idx + ")").hide();
        $(".previewImg:eq(" + idx + ")").show();
        $(".videoWrapper:eq(" + idx + ")").attr("src", "about:blank");
        $(".previewImg:eq(" + idx + ")").attr("src", bigImagePath);
        $(".previewImg:eq(" + idx + ")").attr("title", image_alt);
        $(".title:eq(" + idx + ")").attr("innerHTML", title);
        $(".text:eq(" + idx + ")").attr("innerHTML", description);
        $(".photographer:eq(" + idx + ")").attr("innerHTML", photographer);
        if (title == '') {
            $(".h4ImgTitle:eq(" + idx + ")").hide();
        }
        if (description == '') {
            $(".pImgText:eq(" + idx + ")").hide();
        }
        if (photographer == '') {
            $(".pImgPhotographer:eq(" + idx + ")").hide();
        }
        if (videoPath != "") {
            $("#videoPreviewImage").show();
        }
    }).fadeIn("slow");
}
function HideVideoIcon() {
    $("#videoPreviewImage").hide();
}
function setVideoParams(path, title, idx) {
    var fullPlayer = "<object width='{2}' height='{4}' VIEWASTEXT><param name='movie' value='{0}'></param><param
name='allowFullScreen' value='true'></param><param name='allowscriptaccess' value='never'></param><embed src='{1}'
type='application/x-shockwave-flash' allowscriptaccess='always' allowfullscreen='true' width='{3}' height='{5}'>
</embed></object>";

    var width = 298;
    var height = 200;

    fullPlayer = fullPlayer.replace("{0}", path);
    fullPlayer = fullPlayer.replace("{1}", path);
    fullPlayer = fullPlayer.replace("{2}", width);
    fullPlayer = fullPlayer.replace("{3}", width);
    fullPlayer = fullPlayer.replace("{4}", height);
    fullPlayer = fullPlayer.replace("{5}", height);

    $(".videoWrapper:eq(" + idx + ")").attr("innerHTML", fullPlayer);
}

function ClearVideoParams(idx) {
    $(".videoWrapper:eq(" + idx + ")").attr("innerHTML", "");
}
```

אמצעי נגד:

1. מומלץ להגביל את המאפיין AllowScriptAccess במערכת לפחות להגדרות sameDoamin.
2. במידת האפשר, עדיף להגדיר את המאפיין לערך never.

5. חשיפת גרסת השרת

להלן צילום מסך של חשיפת גרסת השרת:



אמצעי נגד:

1. מומלץ לדאוג להסתיר את המידע בשרת האפליקציה. תהליך מפורט בכתובת:

http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx