

בדיקת חוסן אפליקטיבית – מערכת חיל חימוש

עבור

ממשל זמין



בוצע ע"י:

רעות חכמון

יועצת לאבטחת מידע

2bsecure, The security division of Matrix

© הודעה בדבר זכויות יוצרים: אין להעתיק, לשכתב, לצלם או לשלוח מסמך זה או חלקים ממנו מבלי לקבל אישור בכתב מממשל זמין. המידע המופיע במסמך זה הנו רכושו הבלעדי של ממשל זמין וחברת 2Bsecure. כל הקורא מסמך זה, כולו או מקצתו, ואינו מורשה לצפות במידע המופיע בו, חשוף לתביעה משפטית. המוצא מסמך זה מתבקש להעבירו לידי ממשל זמין, אגף מערכות מידע.

תוכן עניינים

| | |
|----------------|---|
| 2..... | תוכן עניינים |
| 3..... | פרק א' – תקציר מנהלים |
| 3..... | כללי |
| 3..... | תיאור הפעילות |
| 3..... | אילוצים |
| 3..... | התרשמות כללית |
| 4..... | טבלת אינדקס לעיקרי הממצאים והמלצות |
| 5..... | פרק ב' – בדיקת האפליקציה ופרוט הממצאים |
| 5..... | 1. שימוש ברכיבי תוכנה פגיעים |
| 6..... | 2. משתנה VIEW STATE אינו מוצפן |
| 7..... | 3. DEBUG פעיל בצד השרת |
| 8..... | 4. דליפת מידע דרך רכיבי FLASH |
| 9..... | 5. חשיפת גרסת השרת |
| 10..... | 6. שימוש בשם ברירת מחדל של ה-COOKIE |
| 11..... | נספח א – מתודולוגיה ורשימת הבדיקות |
| 11..... | מתודולוגיה |
| 11..... | רשימת המתקפות והבדיקות שבוצעו במהלך הבדיקה: |

12/11/2014

תאריך:

מ.ר. אברהם זרוק

לכבוד:

1211201401

סימוכין:

הנדון: בדיקת חוסן אפליקטיבית – מערכת חיל חימוש**פרק א' – תקציר מנהלים****כללי**

ממשל זמין זימנה את חברת 2Bsecure לבצע בדיקת חוסן למערכת חיל חימוש. מטרת הבחינה הינה למדוד את רמת האבטחה של מערכת חיל חימוש תוך שימת דגש על:

- חוסנה האפליקטיבי של האפליקציה.
- התהליכים העסקיים במערכת.
- התמקדות באיומים הרלוונטיים לטכנולוגית פיתוח האפליקציה.

תיאור הפעילות

במהלך חודש נובמבר 2014 בוצעה בדיקת חוסן אפליקטיבית למערכת חיל חימוש שנמצאת בכתובת: <http://www.chimush.atal.idf.il> המערכת מבוססת Web וכתובה בטכנולוגיית asp ו- NET. אשר רצה על שרת אינטרנט מסוג IIS 6. הבדיקה התבצעה בסוף שלב פיתוח על סביבת יצור.

המידע הרגיש במערכת הינו:

- מידע ארגוני

האיומים העיקרים המיוחסים הינם:

- חשיפת מידע רגיש
- מניעת שירות

אילוצים

- הבדיקה התבצעה מתוך ממשל זמין בהתאם להנחיות ממשל זמין.

התרשמות כללית

מהבדיקה שנערכה התקבל הרושם כי האתר פותח בהתאם לסטנדרטים גבוהים של אבטחת מידע, עם זאת נמצא כי הוא מושתת על שרת החשוף למתקפות רבות. חשיפה למתקפות אלו מסכנת את פעילות המשתמשים באתר ואת המידע אותו האתר מנהל. **נדרש** לשדרג את גרסת האתר.

טבלת אינדקס לעיקרי הממצאים והמלצות

לפניך טבלה המכילה קישורים לכל הממצאים העיקריים בגוף המסמך. ממצאים עיקריים הם כאלו שחומרתם **גבוהה**. ממצאים אלו נבחרו מאחר והם הקריטיים ביותר ביחס לשאר הממצאים ולצורך מתן פרספקטיבה כללית על חוסן המערכת, אין בכך להחליט כי שאר הממצאים אינם דורשים טיפול. יש לעבור על [גוף המסמך](#) לצורך למידת המפגעים והפתרונות שניתנו לכל מפגע ומפגע וליישם במערכת לפי תכנון מסודר.

| מס | ממ\המ | ממצא\המלצה (קישור לגוף המסמך) |
|----|-------|---|
| .1 | ממצא | שימוש ברכיבי תוכנה פגיעים |
| | המלצה | 1. מומלץ לשדרג את גרסת השרת. |

לסיכום, המערכת נכון לעכשיו נמצאת בסיכון **גבוה** למתקפות אפליקטיביות ויש לתקן את הממצאים בהקדם.

פרק ב' - בדיקת האפליקציה ופרוט הממצאים

1. שימוש ברכיבי תוכנה פגיעים

תיאור האיום:

נמצא כי האפליקציה מושתתת על שרת בעל פגיעויות מרובות וידועות. שרת האפליקציה מושתתת על שרת מסוג IIS6. גרסה זו ישנה ובעלת פרצות רבות הידועות לכלל הציבור, ביניהן: הרצת קוד ממחשב מרוחק, השבתת שירות וכדומה.

רמת סיכון:

גבוהה

סיווג STRIDE:

Spoofting - זיוף זהות

Tampering - ביצוע שינוי במידע

Repudiation - הכחשה לביצוע פעולות.

Information Disclosure - חשיפת מידע

Denial of Service - חסימת שירות

Elevation of privilege - שינוי הרשאות והיות של משתמשים

טכניקת המתקפה:

תוקף עלול לחשוף את גרסת השרת, למצוא את חולשותיו המפורטות באינטרנט ולנצלן במטרה להזיק לשרת או לחשוף מידע של הארגון.

התמונה הבאה מציגה את רשימת החולשות של גירסת השרת הנוכחית כפי שמפורסמת באינטרנט:

| # | CVE ID | CWE ID | # of Exploits | Vulnerability Type(s) | Published | Updated | Score | Gained Access Level | Access | Complexity | Authentication | Conf. | Integ. | Avail. |
|---|---------------|--------|---------------|-------------------------------|------------|------------|-------|---------------------|--------|------------|----------------|----------|----------|----------|
| 1 | CVE-2010-1899 | 119 | 1 | DoS Overflow | 2010-09-15 | 2011-07-18 | 4.3 | None | Remote | Medium | Not required | None | None | Partial |
| Stack consumption vulnerability in the ASP implementation in Microsoft Internet Information Services (IIS) 5.1, 6.0, 7.0, and 7.5 allows remote attackers to cause a denial of service (daemon outage) via a crafted request, related to asp.dll, aka "IIS Repeated Parameter Request Denial of Service Vulnerability." | | | | | | | | | | | | | | |
| 2 | CVE-2010-2426 | 24 | 2 | Exec Code Mem. Corr. | 2010-06-08 | 2010-08-21 | 7.5 | Admin | Remote | Medium | Single system | Complete | Complete | Complete |
| Unspecified vulnerability in Microsoft IIS 6.0, 7.0, and 7.5, when Extended Protection for Authentication is enabled, allows remote authenticated users to execute arbitrary code via unknown vectors related to "token checking" that trigger memory corruption, aka "IIS Authentication Memory Corruption Vulnerability." | | | | | | | | | | | | | | |
| 3 | CVE-2009-4448 | 20 | 2 | Exec Code Overflow | 2009-12-29 | 2010-03-18 | 6.0 | User | Remote | Medium | Single system | Partial | Partial | Partial |
| Microsoft Internet Information Services (IIS), when used in conjunction with unspecified third-party upload applications, allows remote attackers to create empty files with arbitrary extensions via a filename containing an initial extension followed by a colon and a safe extension, as demonstrated by an upload of a .asp;.jpg file that results in creation of an empty .asp file, related to support for the HTTP Alternate Data Streams (ADS) filename syntax. NOTE: it could be argued that this is a vulnerability in the third-party product, not IIS, because the third-party product should be applying its extension restrictions to the portion of the filename before the colon. | | | | | | | | | | | | | | |
| 4 | CVE-2009-3844 | 40 | 4 | Bypass | 2009-10-29 | 2010-06-28 | 6.0 | User | Remote | Medium | Single system | Partial | Partial | Partial |
| Microsoft Internet Information Services (IIS) 5.x and 6.x uses only the portion of a filename before a semicolon character to determine the file extension, which allows remote attackers to bypass intended extension restrictions of third-party upload applications via a filename with a (1) .asp, (2) .cer, or (3) .asa first extension, followed by a semicolon and a safe extension, as demonstrated by the use of esp.dll to handle e..asp;.jpg file. | | | | | | | | | | | | | | |
| 5 | CVE-2009-3023 | 119 | 3 | Exec Code Overflow Mem. Corr. | 2009-08-31 | 2011-06-24 | 7.5 | None | Remote | Medium | Not required | Complete | Complete | Complete |
| Buffer overflow in the FTP Service in Microsoft Internet Information Services (IIS) 5.0 through 7.0 allows remote authenticated users to execute arbitrary code via a crafted NLST (NAME LIST) command that uses wildcards, leading to memory corruption, aka "IIS FTP Service RCE and DoS Vulnerability." | | | | | | | | | | | | | | |
| 6 | CVE-2009-2621 | 399 | 6 | DoS | 2009-09-04 | 2011-06-24 | 7.5 | None | Remote | High | Not required | None | None | Partial |
| Stack consumption vulnerability in the FTP Service in Microsoft Internet Information Services (IIS) 5.0 through 7.0 allows remote authenticated users to cause a denial of service (daemon crash) via a tel (ls) -R command containing a wildcard that references a subdirectory, followed by a ; - (dot dot), aka "IIS FTP Service DoS Vulnerability." | | | | | | | | | | | | | | |
| 7 | CVE-2009-1338 | 247 | 7 | Bypass | 2009-06-10 | 2010-08-21 | 7.4 | None | Remote | High | Not required | Complete | Complete | Complete |
| The WebDAV extension in Microsoft Internet Information Services (IIS) 5.1 and 6.0 allows remote attackers to bypass URI-based protection mechanisms, and list folders or read, create, or modify files via a %u002f (Unicode / character) at an arbitrary position in the URL, as demonstrated by inserting %u002f into a "protected" initial pathname component to bypass the password protection on the protected folder, aka "IIS 5.1 and 6.0 WebDAV Authentication Bypass Vulnerability," a different vulnerability than CVE-2009-1122. | | | | | | | | | | | | | | |
| 8 | CVE-2009-1446 | 189 | 8 | Exec Code Overflow | 2008-10-14 | 2009-03-04 | 7.5 | None | Remote | Low | Single system | Complete | Complete | Complete |
| Integer overflow in the Internet Printing Protocol (IPP) ISAPI extension in Microsoft Internet Information Services (IIS) 5.0 through 7.0 on Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, and Server 2008 allows remote authenticated users to execute arbitrary code via an HTTP POST request that triggers an outbound IPP connection from a web server to a machine operated by the attacker, aka "Integer Overflow in IPP Service Vulnerability." | | | | | | | | | | | | | | |
| 9 | CVE-2009-1051 | 19 | 9 | XSS | 2010-02-05 | 2010-02-08 | 6.5 | None | Remote | High | Not required | None | Partial | None |
| Microsoft Internet Information Services (IIS) 6.0, when DNS resolution is enabled for client IP addresses, allows remote attackers to inject arbitrary text into log files via an HTTP request in conjunction with a crafted user-agent string. | | | | | | | | | | | | | | |

אמצעי נגד:

1. מומלץ לשדרג את גרסת השרת.

2. משתנה View State אינו מוצפן

תיאור האיום:

האפליקציה משתמשת במשתנה ה- View State המובנה של טכנולוגיית .NET. ומקודד ב-Base64. משתנה זה מכיל מידע לגבי הדף שמוצג למשתמש, מידע בנוגע לפעילותו ב-Session הקיים ובמקרים רבים מכיל מיד רגיש בנוגע למשתמש. השימוש בערך זה ללא הצפנה עלול לחשוף את פרטי המשתמש למשתמשים זדוניים ובנוסף מסכנת במתקפות מסוג CSRF.

רמת סיכון:

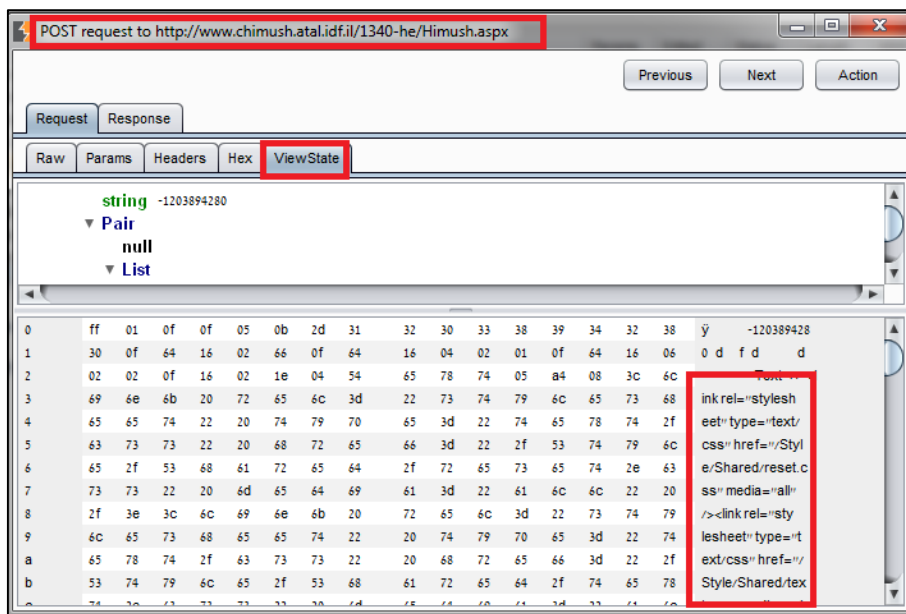
בינונית

סיווג STRIDE:

Information Disclosure - חשיפת מידע

טכניקת המתקפה:

משתמש זדוני אשר צופה בבקשות והתשובות של משתמש אחר עלול לפענח את הערך של משתנה ה View State בהמרה פשוטה (Base64) ולהשתמש בו כנגד המשתמש.



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

3. DEBUG פעיל בצד השרת

תיאור האיום:

בתהליך בניה של אתר מפעילים מתודה שנקראת DEBUG במטרה לעזור ולפתור בעיות במידה וכלאה יוצו.

תוקף אשר משיג פרטי הזדהות לאתר עלול לפנות לדפים עם אפשרות DEBUG ולצפות במידע רגיש על האתר.

כמו כן, תוקף יכול לנסות לשלוח פקודות DEBUG למערכת גם ללא פרטי הזדהות למערכת. במידה ואלה אכן יגיעו לשרת, הדבר יכול להפעיל את אפשרות ה DEBUG בשרת, דבר שצורך משאבים מהשרת ויכול לגרום להאטה משמעותית באתר ואף יצירת מניעת שירות בעקבות כך.

רמת סיכון:

בינונית

סיווג STRIDE:

Information Disclosure - חשיפת מידע

Denial of Service – חסימת שירות

טכניקת המתקפה:

תוקף האוסף מידע על מנת לפגוע באתר מהר מאוד יגלה כי אפשרות ה Debug באתר אינה כבויה. כתוצאה, התוקף יכול לשלוח פקודות Debug לאפליקציה, דבר שיאט אותה משמעותית ויפגע בזמינות האתר.

```

DEBUG /1203-he/AppScan.aspx HTTP/1.1
Command: stop-debug
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://www.chimush.stal.idf.il/994-he/Himush.aspx
Host: www.chimush.stal.idf.il
User-Agent: Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Cookie: ASP.NET_SessionId=gn3nlo55siraouaklrsbix55

HTTP/1.1 200 OK
Date: Wed, 12 Nov 2014 16:50:04 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 2
OK
    
```

אמצעי נגד:

1. מומלץ להוסיף לקובץ ה web.config את הפקודה הבאה:

```

<compilation
debug="false"
/>
    
```

על מנת לנטרל את אפשרות ה debug בסיום פיתוח האתר.

לפרטים נוספים: <http://support.microsoft.com/kb/815157>

4. דליפת מידע דרך רכיבי Flash

תיאור האיום:

לרכיבי ה Flash במערכת ישנם מאפייני אבטחה הרלוונטיים רק אליהם. כאשר המאפיין AllowScriptAccess מוגדר כ Always, המשמעות היא שהאתר סומך רכיב ה Flash והרכיב יכול לגשת לכל מרחב ה DOM של הדפדפן כלומר, לכל החלקי הדפדפן. באופן זה, ניתן באמצעות קובץ Flash זדוני לגשת לערכי ה cookie של משתמש ולגנוב מידע רגיש.

רמת סיכון:

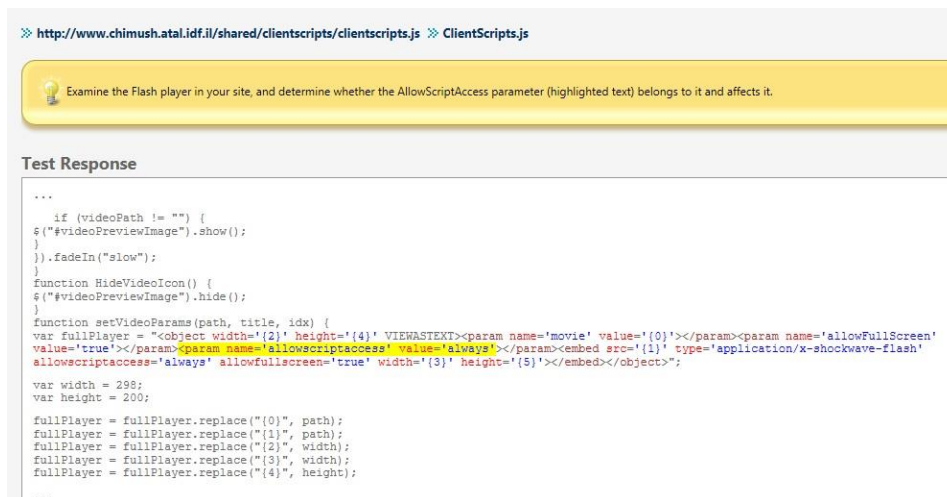
בינונית

סיווג STRIDE:

Information Disclosure - חשיפת מידע

טכניקת המתקפה:

אם המערכת מאפשרת למשתמש להעלות קובץ Flash, תוקף יכול ליצור קובץ Flash זדוני, להעלותו למערכת ולשלוח לחבריו. כתוצאה, רכיב ה Flash יוכל לפעול בחופש מלא בדפדפן כיוון שההגדרה של מאפיין AllowScriptAccess הינו Always. להלן צילום מסך מתוך המערכת המציג הגדרה זו:



```

...
    if (videoPath != "") {
        $("#videoPreviewImage").show();
    }
    }).fadeIn("slow");
}
function HideVideoIcon() {
    $("#videoPreviewImage").hide();
}
function setVideoParams(path, title, idx) {
    var fullPlayer = "<object width='{2}' height='{4}' VLENASTEXT<param name='movie' value='{0}'></param><param name='allowFullScreen' value='true'></param><param name='allowscriptaccess' value='always'></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("{4}", height);
}
...

```

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

תיאור האיום:

השרת חושף למשתמשי הקצה את גרסאות המשאבים שלו. תוקף זדוני עלול לנצל חולשות אשר קיימות בגרסאות הספציפיות ולפרוץ לשרת.

רמת סיכון:

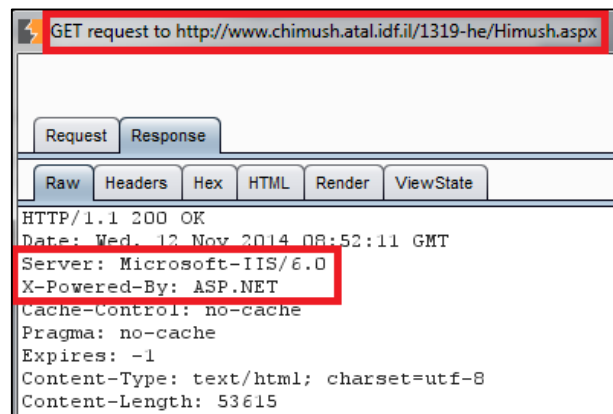
נמוכה

סיווג STRIDE:

Information Disclosure - חשיפת מידע

טכניקת המתקפה:

צפייה בתגובת ה-HTTP החוזרת מהשרת חושפת את גרסת השרת וגרסת הטכנולוגיות של האפליקציה, להלן תמונת מסך של התגובה:



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>

6. שימוש בשם ברירת מחדל של ה-Cookie

תיאור האיום:

המערכת עושה שימוש ב-Cookie עם שם ברירת המחדל של סביבת ה-dotnet. במידה וקיימות אפליקציות נוספות על השרת, אפליקציות אלו יעשו שימוש ב-cookie של מערכת.

רמת סיכון:

נמוכה

סיווג STRIDE:

Spoofting - זיוף זהות

Information Disclosure - חשיפת מידע

טכניקת המתקפה:

במידה וקיימות אפליקציות נוספות על השרת, אשר נתנו את אותו שם ל-cookie, הדפדפן יעשה שימוש באותו ה-cookie בכדי לפנות למערכת ולהפך. להלן מסך המציג את ה-cookie:

```
GET /1203-he/Himush.aspx HTTP/1.1
Host: www.chimush.atal.idf.il
Proxy-Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/38.0.2125.111 Safari/537.36
Referer: http://www.chimush.atal.idf.il/1210-he/Himush.aspx
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8,he;q=0.6,id;q=0.4,ms;q=0.2
Cookie: ASP.NET_SessionId=qe5qgjztzdev4lrdbauf3145; __atuvc=33%7C46;
__atuvs=54633641028226c4017
```

אמצעי נגד:

1. מומלץ לתת שם יחודי ל-Cookie ע"י הוספת ההגדרה הבאה לקונפיגורציה (Web.config):

```
<sessionState cookieName="NAME" />
```

נספח א – מתודולוגיה ורשימת הבדיקות

מתודולוגיה

מתודולוגיית הבדיקות של חברת 2Bsecure מתבססת על מתודולוגיית OWASP הכוללת בדיקות תקיפה נרחבות בכל הנוגע לתחום האפליקטיבי, תוך התמקדות בטכנולוגיית הפיתוח. שיטת הבדיקה מתבססת על בדיקות ידניות תוך שילוב כלים אוטומטיים. אופי הבדיקה מתבסס על גישת Black Box. הייחודיות של בדיקה זו היא הדימוי האמיתי לתוקף (האקר) המנסה לנצל חולשות באפליקציה בכדי לפגוע במשתמשי האפליקציה ומפעיליה. בבדיקה זו ניתן לקבוע באיזה רמת סיכון נמצאת האפליקציה לגבי חדירה של תוקף ללא כל ידע מוקדם על האפליקציה.

רשימת המתקפות והבדיקות שבוצעו במהלך הבדיקה:

לפניך טבלה המכילה את רשימת סוגי המתקפות והבדיקות שמתבצעות ע"י חברת 2bsecure במהלך בדיקות אבטחה. רשימה זו כוללת את כל המתקפות המוכרות נכון לזמן הפקת המסמך. חשוב לציין כי המערכת נמצאה פגיעה למתקפות המפורטות בגוף המסמך ומוגנת (בכפוף למשך ביצוע הפעילות ולאופי הבדיקה יתכן כי ישנם בעיות שקיימות אך לא נחשפו) מפני מתקפות שאינן כלולות בגוף המסמך נכון לזמן ביצוע הבדיקות והפקת המסמך.

| Category | Ref. Number | Test Name | Vulnerability |
|---|--------------|---|--|
| Information Gathering | OWASP-IG-001 | Spiders, Robots and Crawlers - | N.A. |
| | OWASP-IG-002 | Search Engine Discovery/Reconnaissance | N.A. |
| | OWASP-IG-003 | Identify application entry points | N.A. |
| | OWASP-IG-004 | Testing for Web Application Fingerprint | N.A. |
| | OWASP-IG-005 | Application Discovery | N.A. |
| | OWASP-IG-006 | Analysis of Error Codes | Information Disclosure |
| Configuration Management Testing | OWASP-CM-001 | SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity) | SSL Weakness |
| | OWASP-CM-002 | DB Listener Testing | DB Listener weak |
| | OWASP-CM-003 | Infrastructure Configuration Management Testing | Infrastructure Configuration management weakness |
| | OWASP-CM-004 | Application Configuration Management Testing | Application Configuration management weakness |
| | OWASP-CM-005 | Testing for File Extensions Handling | File extensions handling |
| | OWASP-CM-006 | Old, backup and unreferenced files | Old, backup and unreferenced files |

| Category | Ref. Number | Test Name | Vulnerability |
|-------------------------------|--------------|--|--|
| | OWASP-CM-007 | Infrastructure and Application Admin Interfaces | Access to Admin interfaces |
| | OWASP-CM-008 | Testing for HTTP Methods and XST | HTTP Methods enabled, XST permitted, HTTP Verb |
| Authentication Testing | OWASP-AT-001 | Credentials transport over an encrypted channel | Credentials transport over an encrypted channel |
| | OWASP-AT-002 | Testing for user enumeration | User enumeration |
| | OWASP-AT-003 | Testing for Guessable (Dictionary) User Account | Guessable user account |
| | OWASP-AT-004 | Brute Force Testing | Credentials Brute forcing |
| | OWASP-AT-005 | Testing for bypassing authentication schema | Bypassing authentication schema |
| | OWASP-AT-006 | Testing for vulnerable remember password and pwd reset | Vulnerable remember password, weak pwd reset |
| | OWASP-AT-007 | Testing for Logout and Browser Cache Management | Logout function not properly implemented, browser cache weakness |
| | OWASP-AT-008 | Testing for CAPTCHA | Weak Captcha implementation |
| | OWASP-AT-009 | Testing Multiple Factors Authentication | Weak Multiple Factors Authentication |
| | OWASP-AT-010 | Testing for Race Conditions | Race Conditions vulnerability |
| Session Management | OWASP-SM-001 | Testing for Session Management Schema | Bypassing Session Management Schema, Weak Session Token |
| | OWASP-SM-002 | Testing for Cookies attributes | Cookies are set not 'HTTP Only', 'Secure', and no time validity |
| | OWASP-SM-003 | Testing for Session Fixation | Session Fixation |
| | OWASP-SM-004 | Testing for Exposed Session Variables | Exposed sensitive session variables |
| | OWASP-SM-005 | Testing for CSRF | CSRF |
| Authorization Testing | OWASP-AZ-001 | Testing for Path Traversal | Path Traversal |
| | OWASP-AZ-002 | Testing for bypassing authorization schema | Bypassing authorization schema |
| | OWASP-AZ-003 | Testing for Privilege Escalation | Privilege Escalation |
| Business logic testing | OWASP-BL-001 | Testing for business logic | Bypassable business logic |
| | OWASP-DV-001 | Testing for Reflected Cross Site Scripting | Reflected XSS |
| | OWASP-DV-002 | Testing for Stored Cross Site Scripting | Stored XSS |
| | OWASP-DV-003 | Testing for DOM based Cross Site Scripting | DOM XSS |

| Category | Ref. Number | Test Name | Vulnerability |
|----------------------------------|--------------------------------------|------------------------------------|------------------------------------|
| Data Validation Testing | OWASP-DV-004 | Testing for Cross Site Flashing | Cross Site Flashing |
| | OWASP-DV-005 | SQL Injection | SQL Injection |
| | OWASP-DV-006 | LDAP Injection | LDAP Injection |
| | OWASP-DV-007 | ORM Injection | ORM Injection |
| | OWASP-DV-008 | XML Injection | XML Injection |
| | OWASP-DV-009 | SSI Injection | SSI Injection |
| | OWASP-DV-010 | XPath Injection | XPath Injection |
| | OWASP-DV-011 | IMAP/SMTP Injection | IMAP/SMTP Injection |
| | OWASP-DV-012 | Code Injection | Code Injection |
| | OWASP-DV-013 | OS Commanding | OS Commanding |
| | OWASP-DV-014 | Buffer overflow | Buffer overflow |
| | OWASP-DV-015 | Incubated vulnerability Testing | Incubated vulnerability |
| OWASP-DV-016 | Testing for HTTP Splitting/Smuggling | HTTP Splitting, Smuggling | |
| Denial of Service Testing | OWASP-DS-001 | Testing for SQL Wildcard Attacks | SQL Wildcard vulnerability |
| | OWASP-DS-002 | Locking Customer Accounts | Locking Customer Accounts |
| | OWASP-DS-003 | Testing for DoS Buffer Overflows | Buffer Overflows |
| | OWASP-DS-004 | User Specified Object Allocation | User Specified Object Allocation |
| | OWASP-DS-005 | User Input as a Loop Counter | User Input as a Loop Counter |
| | OWASP-DS-006 | Writing User Provided Data to Disk | Writing User Provided Data to Disk |
| | OWASP-DS-007 | Failure to Release Resources | Failure to Release Resources |
| | OWASP-DS-008 | Storing too Much Data in Session | Storing too Much Data in Session |
| Web Services Testing | OWASP-WS-001 | WS Information Gathering | N.A. |
| | OWASP-WS-002 | Testing WSDL | WSDL Weakness |
| | OWASP-WS-003 | XML Structural Testing | Weak XML Structure |
| | OWASP-WS-004 | XML content-level Testing | XML content-level |
| | OWASP-WS-005 | HTTP GET parameters/REST Testing | WS HTTP GET parameters/REST |
| | OWASP-WS-006 | Naughty SOAP attachments | WS Naughty SOAP attachments |
| | OWASP-WS-007 | Replay Testing | WS Replay Testing |
| AJAX Testing | OWASP-AJ-001 | AJAX Vulnerabilities | N.A |
| | OWASP-AJ-002 | AJAX Testing | AJAX weakness |