בדיקת חוסן אפליקטיבית – מערכת הגנת הסביבה

עבור

ממשל זמין

בוצע ע"י:

צוות בדיקות חוסן

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.

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

תוכן עניינים 2

פרק א' – תקציר מנהלים 3

כללי 3

תיאור הפעילות 3

אילוצים 3

התרשמות כללית 3

טבלת אינדקס לעיקרי הממצאים והמלצות 4

פרק ב' - בדיקת האפליקציה ופרוט הממצאים 5

1. שימוש ברכיבי תוכנה פגיעים 5
2. משתנה VIEW STATE אינו מוצפן 7
3. חשיפת גרסת השרת 8
4. שימוש בשם ברירת מחדל של ה-COOKIE 9

נספח א– מתודולוגיה ורשימת הבדיקות 10

מתודולוגיה 10

רשימת המתקפות והבדיקות שבוצעו במהלך הבדיקה: 10

לכבוד: מר. אברהם זרוק **תאריך:** **13/11/2014**

סימוכין: **1311201401**

הנדון: בדיקת חוסן אפליקטיבית –מערכת הגנת הסביבה

פרק א' – תקציר מנהלים

כללי

ממשל זמין זימנה את חברת 2Bsecure לבצע בדיקת חוסן למערכת הגנת הסביבה.

מטרת הבחינה הינה למדוד את רמת האבטחה של מערכת הגנת הסביבה 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.hagnas.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.

<u>המידע הרגיש במערכת הינו:</u>

- מידע ארגוני

<u>האיומים העיקרים המיוחסים הינם:</u>

- חשיפת מידע רגיש
- מניעת שירות

אילוצים

- הבדיקה התבצעה מתוך ממשל זמין בהתאם להנחיות ממשל זמין.
- דף צור קשר אינו פעיל במערכת ולכן לא נבדק.

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

לפנייך 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. הנחיות ליישום ההמלצות יינתנו לפי צורך ובהתאם בתכולת הבדיקה.

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.

רמת סיכון:

גבוהה

סיווג STRIDE:

Spoofing- זיוף זהות

Tampering- ביצוע שינוי במידע

Repudiation- הכחשה לביצוע פעולות.

Information Disclosure - חשיפת מידע

Denial of Service– חסימת שירות

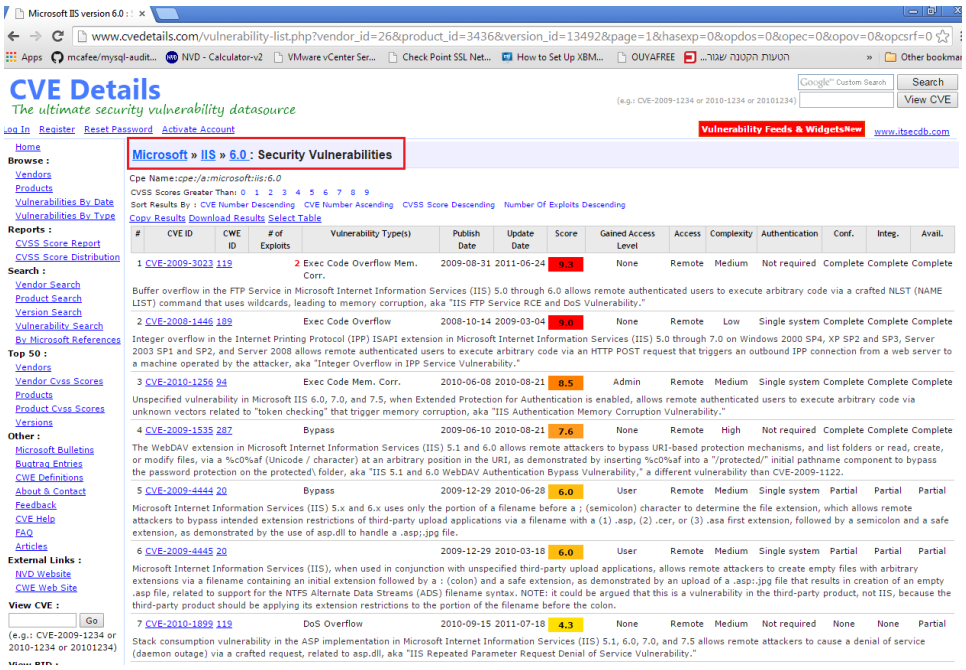
Elevation of privilege- שינוי הרשאות וזהויות של משתמשים

טכניקת המתקפה:

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

להלן צילום מסך המציג זיהוי של גרסת השרת הפועלת בצד המערכת:

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



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 בSession הקיים ובמקרים רבים מכיל מידע רגיש בנוגע למשתמש. השימוש בערך זה ללא הצפנה עלול לחשוף את פרטי המשתמש למשתמשים זדוניים ובנוסף מסכנת במתקפות מסוג CSRF.

רמת סיכון:

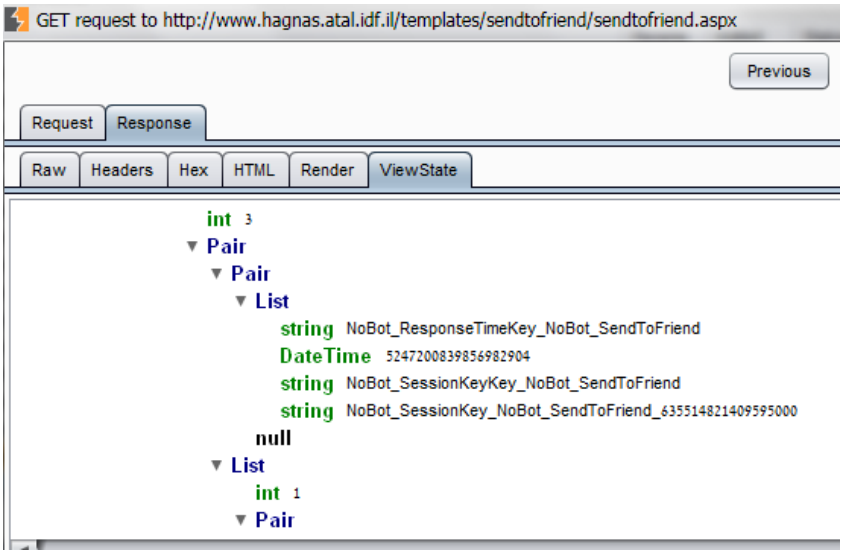
בינונית

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.
בנוסף ניתן לקבל מידע על השרת ועל אופן פעולתו.
להלן צילום מסך המציג את הממצא:



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

3. 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:

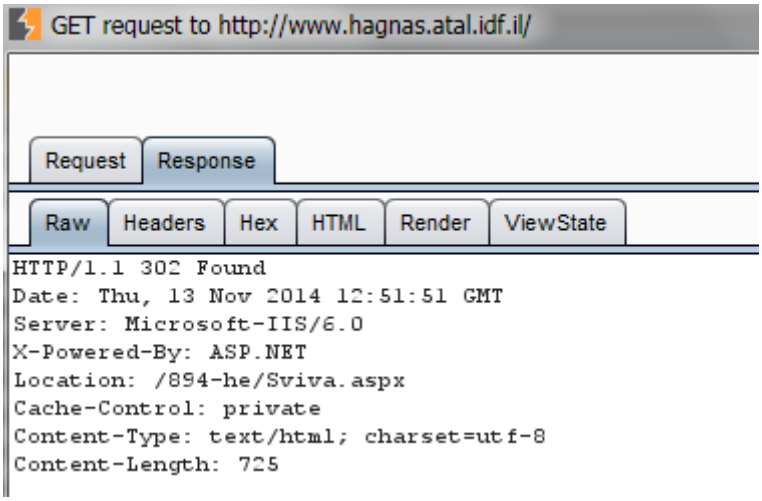
נמוכה

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

4. 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:

Spoofing- 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 /894-he/Sviva.aspx HTTP/1.1
Host: www.hagnas.atal.idf.il
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: __atuvc=11%7C46; ASP.NET_SessionId=irfa4i45vfcrui45uptkynfc; __atuvs=5464a03a42edd9a1007
Connection: keep-alive
```

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

מתודולוגית הבדיקות של חברת 2Bsecure מתבססת על מתודולוגיית OWASP הכוללת בדיקות תקיפה נרחבות בכל הנוגע לתחום האפליקטיבי, תוך התמקדות בטכנולוגית 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