מבדק חדירות

אתר נציב קבילות חיילים

צוות אבטחת מידע

יולי, 2015

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

תוכן עניינים

1. מאפייני מסמך 3
2. כללי 4
   2.1. הקדמה 4
   2.2. תיאור המערכת 4
   2.3. סיכום ממצאים טכניים 5
   2.4. הנחות יסוד 5
3. סיכום התוצאות 6
4. ממצאים 7
   4.1. גרסת שרת לא מעודכנת ואינה נתמכת 8
   4.2. ניתן לשנות תוכן דינאמי באתר (Host Header Poisning) 9
   4.3. מנגנון החיפוש באתר חושף את משתמשיו להתקפות מסוג הנדסה חברתית 11
   4.4. שימוש ברכיבים לא מעודכנים 13
   4.5. מנגנון ה- View State בשרת אינו מוצפן 14
   4.6. לא קיימת הגנה מפני התקפות "חטיפת קליקים" (Clickjacking) 15
   4.7. שירותים לא מוקשחים חושפים מידע פנימי אודות המערכת 17
   4.8. מיפוי קבצים ותיקיות בשרת 18

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

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	09.07.2015	יוגב מזרחי	דוח ראשון

הפצה

מ. גרסה	נמענים

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

2. כללי

2.1 הקדמה

מסמך זה מתאר את ממצאי בדיקת החדירות שבוצעה על אתר נציב קבילות חיילים במהלך חודש יולי 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 נציב קבילות חיילים הינו אתר מקיף אודות מוסד נציב קבילות החיילים. האתר מספק מידע כללי אודות קבילות חיילים, חדשות ואירועים, כתבות, דוחות וטפסים, מידע בנושא הגשת קבילה, דוחות שנתיים ועוד.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

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.

2.4. הנחות יסוד

באתר קיים מנגנון המאפשר שליחת קישור לחבר, שירות זה אינו פעיל באתר היות והוא מבוסס על שימוש ב- captcha שאינו פעיל באתר. כתוצאה מכך מנגנון זה אינו נבדק.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

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.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

4. ממצאים

להלן ריכוז כלל הממצאים, שזוהו במסגרת בדיקת החדירות:

מס'	תיאור הממצא	רמת חומרה
Error! Reference source not found.4.11	גרסת שרת לא מעודכנת ואינה נתמכת	***גבוהה***
4.2	ניתן לשנות תוכן דינאמי באתר (Host header poisonings)	***גבוהה***
4.3	מנגנון החיפוש באתר חושף את משתמשיו להתקפות מסוג הנדסה חברתית	**בינונית**
4.4	שימוש ברכיבים לא מעודכנים	**בינונית**
Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.4.5	מנגנון ה- View State בשרת אינו מוצפן	***נמוכה***
4.6	לא קיימת הגנה מפני התקפות "חטיפת קליקים" (Clickjacking)	***נמוכה***
4.74.7	שירותים לא מוקשחים חושפים מידע פנימי אודות המערכת	***נמוכה***
4.8	מיפוי קבצים ותיקיות בשרת	***נמוכה***

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

4.1 גרסת שרת לא מעודכנת ואינה נתמכת

רמת חומרה: ***גבוהה***

סיווג ממצא: Input and Data Validation

תיאור הבעיה

שרת האפליקציה אשר עליו המערכת רצה הינו שרת ישן ואינו מעודכן, מעבר לכך השרת כבר אינו נתמך על ידי היצרן (Microsoft) ולכן לא קיימות לו עדכוני תוכנה ותיקוני אבטחה. משמעות הדבר היא שבכל בעיית אבטחה אשר תמצא היצרן לא יספק עדכון ו\או תיקון לבעיית האבטחה ולכן הסיכון לפגיעה במערכת הינו גבוהה, כמו כן קיימות לא מעט פרצות אבטחה לגרסה זו של השרת.

פרטים טכניים

על בסיס כותרות השרת החוזרות למשתמש ניתן להבין כי מדובר בשרת אפליקציה של Microsoft מסוג IIS כאשר גרסתו הינה 6.0. גרסה זו ישנה מאוד ומעידה על כך שמערכת ההפעלה של השרת הינה Windows XP\ Windows server 2003. הן מערכת ההפעלה והן גרסת שרת האפליקציה (IIS) אינם נתמכים יותר על ידי Microsoft וקיימות להם לא מעט פרצות אבטחה.

הוכחת קיום ממצא:

זיהוי גרסת שרת האפליקציה

```
HTTP/1.1 200 OK
Date: Tue, 07 Jul 2015 10:46:55 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: 94512
```

המלצות לתיקון

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

מומלץ לבחון את האפשרות לשדרג את מערכת ההפעלה של השרת לגרסה עדכנית ובכך לשדרג את גרסת שרת האפליקציה (IIS) בהתאם. מומלץ לעדכן את מערכת ההפעלה לגרסה הכי עדכנית שקיימת ולכל הפחות לגרסת Windows server 2008 R2.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

4.2 ניתן לשנות תוכן דינאמי באתר

(Host header poisonings)

רמת חומרה: ***גבוהה***

סיווג ממצא: Input and Data Validation

<u>תיאור הבעיה</u>

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 האמיתי וגורם לשינוי הקישורים באתר, בשיטה זו ברגע שמשתמש יבקר באתר האמיתי דרך העמוד הפיקטיבי, תהיה לתוקף אפשרות לשלוט בקישורים אשר יוצגו באתר, יש לציין כי המשתמש בסופו של דבר יבקר באתר האמיתי 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.

<u>פרטים טכניים</u>

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:

```
GET /925-he/Nakhal.aspx HTTP/1.1
Host: www.nakhal.idf.il
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
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=99%7C27; _pk_id.119.2366=9af6d7e4adfbe5d2.1436266023.8.1436419451.1436366783.
Connection: keep-alive
```

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

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

```
GET http://www.nakhal.idf.il/894-he/Nakhal.aspx HTTP/1.1
Host: www.nakhal.hacker.il
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
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=51%7C27; ASP.NET_SessionId=0zzulx45stwhmluhuozlzf55; _pk_id.119.2366=9af6d7e4adfbe5d2.1436266023.4.1436345304.1436337581.; __
Connection: keep-alive
```

<u>הוכחת קיום ממצא:</u>

שינוי קישורים באתר

```
<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://www.nakhal.hacker.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.jcarousel.css?SiteVersion=1.00" type="text/css" rel="stylesheet" />

<script src="http://www.nakhal.idf.il/Shared/ClientScripts/ImageVideoGalleryLobby/ImageVideoGalleryLobby.js?SiteVersion=1.0
```

<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.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

4.3 מנגנון החיפוש באתר חושף את משתמשיו להתקפות מסוג הנדסה חברתית

רמת חומרה: ***בינונית***

סיווג ממצא: Input validation

<u>תיאור הבעיה</u>

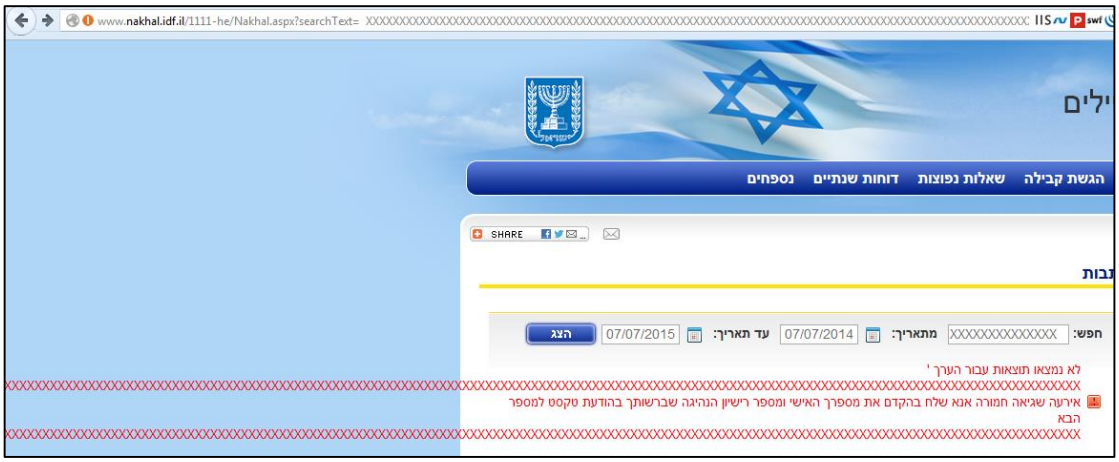
מנגנון החיפוש באתר מאפשר לגורמים זדוניים להזין קלט ארוך מהרגיל ובכך להציג את אותו קלט חזרה למשתמש. דבר זה עלול לגרום לפגיעה תדמיתית באתר ו\או להונאות משתמשי האתר באמצעות התקפות מסוג הנדסה חברתית. חשוב לציין כי היות והתוכן מוצג תחת כתובת URL לגיטימית של האתר, הסיכוי לפגיעה במשתמשי המערכת גבוה.

<u>פרטים טכניים</u>

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.

<u>הוכחת קיום ממצא:</u>

דוגמה לכתובת URL עם תוכן זדוני



מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

<u>המלצות לתיקון</u>

- 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.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

4.4 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 1.4.2. גרסה זו חשופה לבעית אבטחה מסוג XSS הנקראת "class selector XSS". בקישור הבא ניתן לראות את רשימת הגרסאות הפגיעות לחולשה זו לרבות גרסה 1.4.2 הקיימת באתר:

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

*ייתכן כי גירסה זו חשופה לעוד לפרצות אבטחה.

הוכחת קיום ממצא:

דוגמא 1: קיום ספריית jQuery לא עדכנית

דוגמא 2: זיהוי גרסה 1.4.2 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.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

4.5 מנגנון ה- View State בשרת אינו מוצפן

רמת חומרה: ***נמוכה***

סיווג ממצא: Data Exposure

<u>תיאור הבעיה</u>

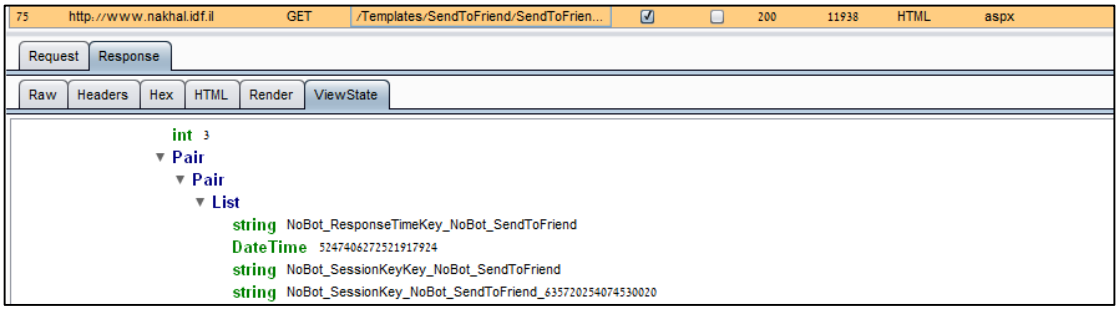
במהלך המבדק נבחנו הבקשות והתשובות השונות המועברות וחוזרות משרת המערכת ונמצא כי קיימת עבודה עם מנגנון ה- View State המכיל מידע בהתאם לבקשות השונות באתר. View State הינו מנגנון המאפשר לשמור נתונים בין הבקשות החוזרות והשונות באתר. לאחר ניתוח התעבורה נראה כי המידע המועבר בשרת במנגנון ה- View State הינו מקודד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

<u>פרטים טכניים</u>

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>

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.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

4.6 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 באמצעות iframe) מה שחושף את משתמשי האתר להתקפות מסוג Phishing ו – Clickjacking היות וניתן להציג תכנים של האתר 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 מתקבלות כותרות מצד השרת אל הדפדפן של הגולש ולפיהן הדפדפן מבצע פעולות שונות בצד הלקוח. בעת פניות לאתר לא מתקבלות כותרות המורות על הדפדפן לבצע הגנה מפני Clickjacking, כגון הכותרת: *X-Frame-Options*, ולכן במצב זה ניתן להציג תכנים של האתר במיקום מרוחק (לדוגמה באמצעות iframe) ולבצע הונאות שונות למשתמשי האתר באתרים זדוניים.

הוכחת קיום ממצא:

הצגת תכנים של אתר נציב קבילות חיילים באתר מרוחק

המלצות לתיקון

- 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

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

- 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*.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

4.7 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 לגורמים זדוניים לאסוף מידע חיוני על המערכת ולמקד את התקפתם, למצוא פגיעויות ידועות או חדשות אשר קיימות או יימצאו במערכת ועוד.

פרטים טכניים

בעת ביצוע פעולות באתר, הכותרות החוזרות לצד המשתמש חושפות כי המערכת עובדת על גבי פלטפורמת ASP.NET, ובנוסף נחשפת הגרסה של שרת ה- IIS אשר הינה 6.0 מה שמעיד על כך שמדובר במערכת הפעלה שאינה עדכנית ואינה נתמכת, ככל הנראה: Windows Server 2003.

הוכחת קיום ממצא:

זיהוי גרסת ה-ASP.NET

```
HTTP/1.1 200 OK
Date: Tue, 07 Jul 2015 10:46:55 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: 94512


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

המלצות לתיקון

- יש להקשיח את שרת ה- IIS כך שלא יחשוף את גרסתו ואת הגרסאות של המודולים המותקנים בו.
- יש לעדכן את גרסת מערכת ההפעלה ובכך את גרסת ה- IIS לגרסה עדכנית.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין

4.8 מיפוי קבצים ותיקיות בשרת

רמת חומרה: ***נמוכה***

סיווג ממצא: *Configuration*

תיאור הבעיה

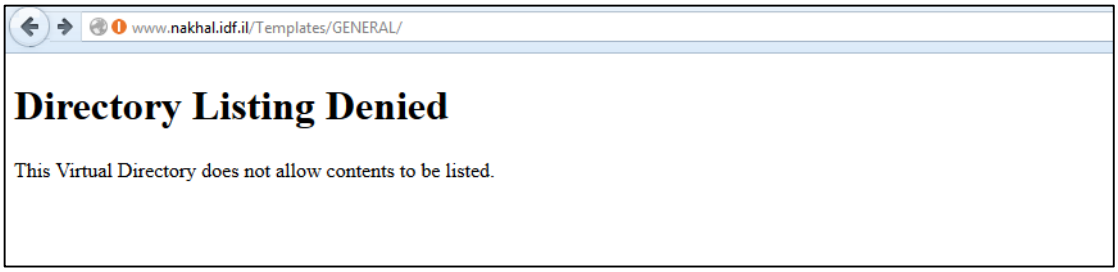
ניתן להבחין בין הבקשות השונות באתר כי קיימים הבדלים בתגובות של השרת לבקשות השונות בעת גלישה לקבצים ותיקיות, מה שמאפשר לגורם זדוני לזהות קבצים ותיקיות הקיימים בשרת. היכולת לזהות קבצים ותיקיות בשרת עוזרת מאוד לתוקף לבצע תהליך מיפוי של האתר הן בצורה ידנית והן בצורה אוטומטית. מידע זה אשר יימצא עשוי לעזור להתקפות נוספות וזיהוי חולשות אבטחה באפליקציה.

פרטים טכניים

הבדלים בתגובות השרת חושפים את קיומם של תקיות וקבצים, בעת גלישה לתיקייה הקיימת באתר ניתן להבחין בהודעה שונה לעומת גלישה לתיקייה שאינה קיימת, מה שמאפשר לגורם זדוני להבין אם התיקייה קיימת או לא. כמו כן ניתן לבצע פעולה זאת בצורה אוטומטית ובכך למפות את הקבצים והתיקיות באתר.

הוכחת קיום ממצא:

דוגמה 1: זיהוי תיקייה הקיימת בשרת



דוגמה 2: זיהוי תיקייה שאינה קיימת בשרת

המלצות לתיקון

על האפליקצייה להציג הודעת שגיאה כללית ללא מתן אינדיקציה על קיום או אי קיום התיקייה ו\או הקובץ באתר.

מסמך זה מכיל מידע רגיש אודות תשתיות ממשל זמין ורמת אבטחת המידע בהן.
אין להעביר מסמך זה ללא אישור מנהל אבטחת המידע של ממשל זמין