מבדק חדירות

אתר אישורים צבאיים

צוות אבטחת מידע

יוני, 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	11.06.2015	יוגב מזרחי	דוח ראשון

הפצה

מ. גרסה	נמענים

2. כללי

2.1 הקדמה

מסמך זה מתאר את ממצאי בדיקת החדירות שבוצעה על אתר אישורים צבאיים במהלך חודש יוני 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 אישורים צבאיים מספק אישורים המציגים פרטים על מהלך השירות הצבאי של חייל אשר משרת בהווה או שרת בעבר בצה"ל. את האישורים ניתן להזמין דרך אתר זה ולקבל בדואר ישירות אל הכתובת המופיעה ברישומי צה"ל, זאת בתנאי והחייל עומד בתנאים להזמנת אישורים. במעמד הזמנת אישור צבאי ניתן לספק כתובת חלופית לשליחת האישורים (כתובת אשר אינה מופיעה במערכת הצבאית). האתר מספק לכל משתמש הזמנה של עד 3 אישורים בחודש. על מנת להיכנס למערכת יש להכניס את הפרטים הבאים:

- מספר אישי
- תאריך לידה
- מספר תעודה צבאית או רשיון נהיגה.

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.Error! Reference source not found. 4.1	Insecure cookie	**בינונית**
4.2	שימוש ב- SSL לא מאובטח	**בינונית**
Error! Reference source not found. 4.34.3	שימוש ברכיבים לא מעודכנים	**בינונית**
4.44.44.4	לא קיימת הגנה מפני התקפות "חטיפת קליקים" (Clickjacking)	**בינונית**
4.54.54.5	מנגנון ה- View State בשרת אינו מוצפן	***נמוכה***
Error! Reference source not found. 4.6	אי טיפול בהודעות שגיאה גורם לחשיפת מידע פנימי של המערכת	***נמוכה***
4.7	מיפוי קבצים ותיקיות בשרת	***נמוכה***

4.1. Insecure cookie

רמת חומרה: ***בינונית***

סיווג ממצא: *Configuration*

תיאור הבעיה

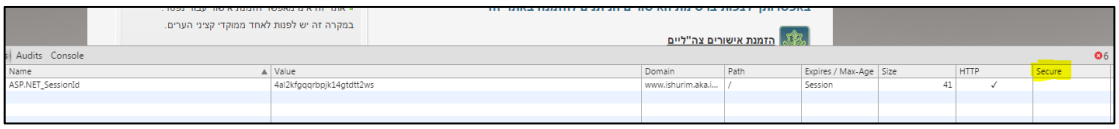
המערכת אינה מגנה כנדרש על מזהה ה- Session הייחודי של משתמשי המערכת הנמצא ב-cookie ומאפשרת לתוקף לגנוב אותו על גבי תווך לא מוצפן. לאחר שהתוקף משיג ה-cookie של המשתמש ועל ידי כך את ה- Session-ID של משתמש הוא יוכל להתחזות באופן מוחלט לאותו משתמש, לבצע פעולות ומתקפות בשמו ובהרשאותיו. התוקף בנוסף יכלול לבצע התקפות שונות מסוג הנדסה חברתית במטרה לגנוב cookies של משתמשים.

פרטים טכניים:

לאחר הזדהות למערכת, השרת מספק למשתמש מזהה ייחודיי (Session ID) הנשמר ב-Cookies כדי למנוע כניסה מחודשת ושמירת נתונים במהלך השימוש באתר. בעת קביעת ה- Cookie על ידי השרת (Set-Cookie) לא הוגדר מאפיין (secure) המורה על כך שלא יהיה ניתן להשתמש ב- cookie ללא תווך מוצפן.

הוכחת קיום ממצא:

דוגמא 1: אי קיום פרמטר ה- secure ב- cookie



המלצות לתיקון

יש להגדיר את מאפיין ה- secure על ה- cookie המכיל את ה- session id של המשתמש.

4.2 שימוש ב- SSL לא מאובטח

רמת חומרה: ***בינונית***

סיווג ממצא: *Configuration*

תיאור הבעיה

האתר עובד על גבי תווך מוצפן (HTTPS), יישום הצפנת התווך נעשה באמצעות פרוטוקולים ישנים (TLS 1.0) ואינו תומך בשימוש פרוטוקולים חדשים ומאובטחים יותר (TLS 1.2). נוסף על כך תעודת ה- SSL חתומה באמצעות אלגוריתם ישן ופגיע (SHA 1).

פרטים טכניים

שרת המערכת תומך בעבודה עם פרוטוקול TLS 1.0 בלבד שהינו פרוטוקול ישן ומכיל בעיות אבטחה. כיום (נכון לכתיבת דוח זה) הפרוטוקול המאובטח ביותר הינו TLS 1.2, שאינו נתמך כרגע בשרת כלל. בנוסף חתימת תעודת ה- SSL הינה באמצעות אלגוריתם ישן מסוג SHA 1 שנחשב כיום כאינו מאובטח מספיק ומכיל בעיות אבטחה.

הוכחת קיום ממצא:

דוגמא 1: תוצאות בדיקת SSL המעידות על שימוש בפרוטוקול ישן

Configuration

Protocols

TLS 1.2	No
TLS 1.1	No
TLS 1.0	Yes
SSL 3	No
SSL 2	No

דוגמא 2: תוצאות בדיקת SSL המעידות על שימוש באלגוריתם חלש

Authentication

Server Key and Certificate #1

Common names	www.ishurim.aka.idf.il
Alternative names	www.ishurim.aka.idf.il
Prefix handling	Not required for subdomains
Valid from	Mon, 31 Oct 2011 08:59:52 UTC
Valid until	Tue, 01 Nov 2016 02:18:59 UTC (expires in 1 year and 4 months)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	GeoTrust DV SSL CA
Signature algorithm	SHA1withRSA **WEAK**

<u>המלצות לתיקון</u>

- מומלץ ליישם את הצפנת התעבורה על גבי הפרוטוקול המאובטח ביותר שניתן כגון TLS 1.2 ולחסום את האפשרות לעבודה עם פרוטוקולים ישנים יותר.
- מומלץ להשתמש באלגוריתם מאובטח יותר בתעודת ה- SSL כגון SHA 2.

4.3 שימוש ברכיבים לא מעודכנים

רמת חומרה: ***בינונית***

סיווג ממצא: *Configuration*

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 (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

פרטים טכניים

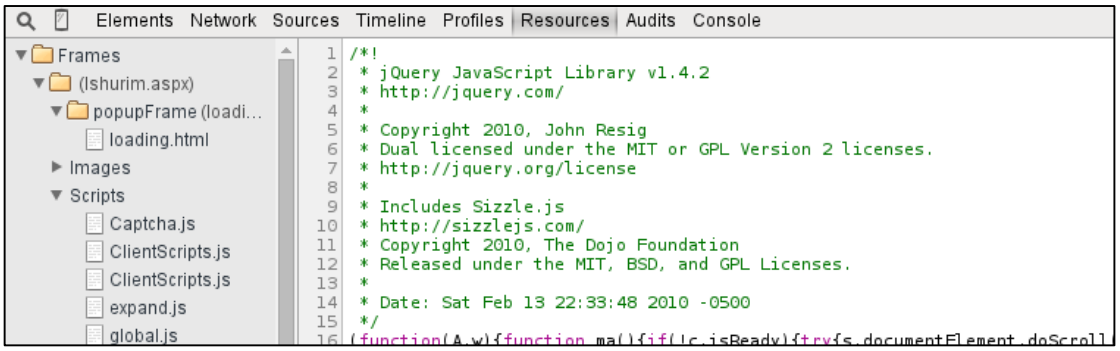
כחלק מבדיקות המערכת נמצא כי נעשה שימוש באתר בספריית jQuery בגרסה ישנה, הגרסה בה נעשה שימוש הינה 1.4.2. היות וגרסה זו חשופה לבעיות אבטחה מסוג XSS, באפשרות גורם זדוני להכין עמוד פיקטיבי אשר גורם להרצה מרוחק של קובץ הג'אווה סקריפט של ספריית ה- jQuery הקיים באתר בנתיב הבא:

https://www.ishurim.aka.idf.il/Shared/ClientScripts/Jquery/jquery-1.4.2.min.js

ולהריץ קוד זדוני בצד הלקוח.

הוכחת קיום ממצא:

דוגמא 1: קיום גרסה ישנה של jquey 1.4.2



המלצות לתיקון

יש לבחון שדרוג של כל המודולים והתוספים באתר לגרסאות האחרונות בכדי להוריד את הסיכון לפגיעה במערכת. יש לעדכן לגרסה הכי עדכנית שניתן.

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 אישורים צבאיים 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 אישורים צבאיים 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
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 50209
Content-Type: text/html; charset=utf-8
Expires: -1
X-Powered-By: ASP.NET
```

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 האישורים צבאיים באתר מרוחק ולבצע הונאות שונות למשתמשי האתר באתרים זדוניים.

<u>הוכחת קיום ממצא:</u>

דוגמא 1: הצגת תכנים של אתר אישורים צבאיים 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 לכולם
  - 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 ה- Deny.

4.5 מנגנון ה- View State בשרת אינו מוצפן

רמת חומרה: נמוכה

סיווג ממצא: *Data Exposure*

תיאור הבעיה

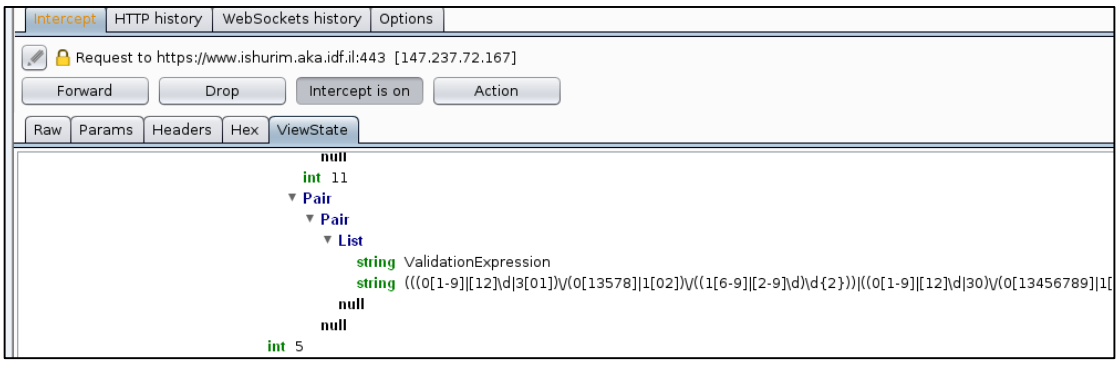
במהלך המבדק נבחנו הבקשות והתשובות השונות המועברות וחוזרות משרת המערכת ונמצא כי קיימת עבודה עם מנגנון ה- View State המכיל מידע בהתאם לבקשות השונות באתר. View State הינו מנגנון המאפשר לשמור נתונים בין הבקשות החוזרות והשונות באתר. לאחר ניתוח התעבורה נראה כי המידע המועבר בשרת במנגנון ה- View State הינו מקודד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

פרטים טכניים

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.

הוכחת קיום ממצא:

דוגמא 1: זיהוי מידע במנגנון ה- View State



המלצות לתיקון

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

```
ViewStateEncryptionMode="Always"
```

ובכך המידע המועבר שם יועבר תמיד בצורה מוצפנת.

4.6. אי טיפול בהודעות שגיאה גורם לחשיפת מידע פנימי של המערכת

רמת חומרה: ***נמוכה***

סיווג ממצא: *Configuration*

תיאור הבעיה

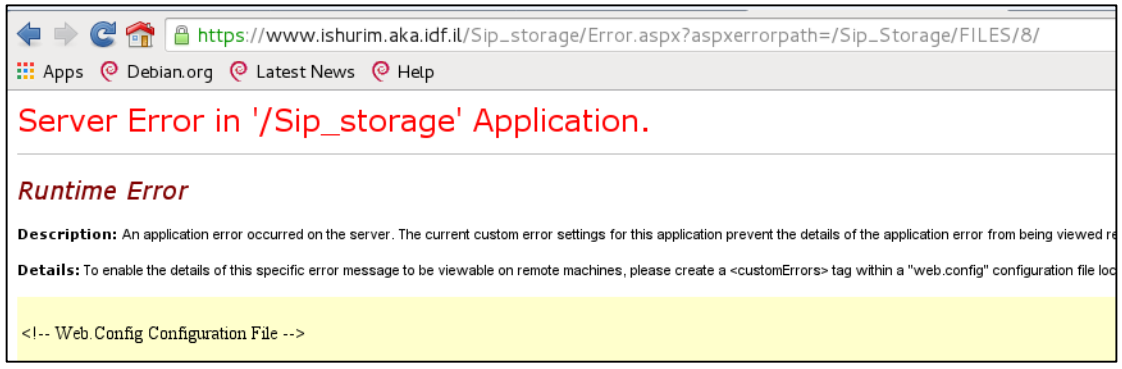
במהלך הגלישה באתר נמצא כי המערכת אינה מטפלת בשגיאות בצורה עקבית ותקינה, ולכן נחשפות הודעות שגיאה המכילות מידע רגיש. גורם זדוני עלול לנצל לרעה את חשיפת המידע בכדי ללמוד את מבנה המערכת. לימוד והיכרות המערכת הינו שלב בסיסי ומקדים לביצוע התקפות על המערכת ועשוי לעזור מאוד לגורם זדוני. השגת מידע על המערכת עוזרת במציאת חשיפות ובעיות אבטחה ידועות ושאינן ידועות הנובעות מהטכנולוגיות המוטמעת בשרת.

פרטים טכניים

המערכת אינה מוגדרת להציג הודעת שגיאה כללית ואחידה המוגדרת מראש ושאינה חושפת מידע ועל כן הודעות שגיאה ישירות של השרת חוזרות אל המשתמש וחושפות לו מידע מורחב אודות התקלה.

הוכחת קיום ממצא:

דוגמה 1: חשיפת שגיאת שרת אל המשתמש



המלצות לתיקון

- יש לייצר עמוד שגיאה כללי שאינו חושף מידע מיותר למשתמש אודות השגיאה.
- יש ללכוד את כל הודעות השגיאה באפליקציה ולהפנותן לעמוד השגיאה הכללי בעת ההתרחשות.

4.7 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 שממאפשר 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.

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.