

דו"ח מסכם פרויקט בבדיקה אבטחה



דוד דרס 305312183

כפיר ליזרוביץ' 313249344

הפקולטה למדעי המחשב

סמסטר חורף תשפ"ב

## הקדמה

בשנים האחרונות אנו עדים לעלייה מתמדת בהיקף ניסיונות התקיפה במרחב הקיברנטי. היכולת לנצל חולשה ב망 שפתו לאינטרנט ולבצע מתקפה שכוללת גניבת מידע השחתה\שינוי מידע אינה נחלתם של מעצמות אלא כל אדם בעל דפדפן, חיבור לאינטרנט וידע בסיסי עלולים להוות גורם מאיים. לשם כך, נדרש לוודא באופן תדיר ומكيف כי מערכות הארגון מגנות היטב.

בפרט, נדרש מיקוד במערכות החשופות לאינטרנט או מערכות הנגישות בראשת פניםית בעלת משתמשים רבים, שלא בהכרח ניתן לסמן עליהם (כדוגמת כל סטודנט הרשות לטכניון, שיש לו גישה לרשות הפניםית)

בפרויקט הנוכחי התמקדנו בכל הנוגע למערכת הציונים הטכניונית Grades, המהווה נכס דיגיטלי חשוב שפגיעה באמינותו או הדלפת מידע ממנו עלולה לגרום נזק רב הן לסטודנטים והן לתדמית הטכניון.

בדוח זה נתאר את ממצאי הבדיקה שביצענו, מיפוי נקודות החולשה והמלצות להמשך.

## רקע

### מבנה מערכת הציונים הטכנית:

מערכת הציונים בטכניון מופרדת ל-2 יישיות נפרדות:

1. **מערכת Grades** – מערכת המיעדת עבור הסטודנטים ומאפשרת צפיה בציונים, היסטוגרמות ובסיקות המבחנים של הסטודנט בקורסים אליו הם רשום.

מערכת זו פותחה לאינטרנט באופן חופשי ומוגנת בשם משתמש וסיסמה המשמשים כהזהות בטכניון.

2. **מערכת Upgrade** – מערכת המיעדת עבור סגל המרצים בקורסים השונים ומאפשרת הזנת ציונים והעלאת סיקות של מחברות המבחנים.

מערכת זו נגישה אך ורק מתוך הרשות הפנימית הטכנית (נדרשת יכולת חיבור לרשת, לדוגמא על-ידי חיבור VPN או התחברות מחשב המחבר לרשות בתוך הטכניון), ויש לה 2 סביבות: סביבת-hsproduction שבה משתמשים בפועל, וסביבת develop שעליה נעשות בדיקות אינטגרציה לפי ביצוע שינויים בפונקציונליות של המערכת הראשית.

כמו כן, קיים אתר מיושן המאפשר צפיה בתדריס הציונים עליו נפרט בהמשך.

### ממשקים נוספים:

וDU – שירות הנitinן לסטודנטים המאפשר התחברות למcona וירטואלית לטובת משאבי מחשב.

CSL3, CSCOM – שירותי של הפקולטה למדעי המחשב הנמצאים ברשות הטכנית ונגישים לסטודנטים בפקולטה.

הכליים העיקריים שעבדנו איתם לצורך ביצוע בדיקת האבטחה היו, `burpsuite`, `wireshark`, `mapreduce` ו-`metasploit`. סביבת העבודה העיקרי הייתה מערכת הפעלה של `unix` שעלה הותקן `kali`.

## סקירת ספרות

:OWASP TOP 10<sup>1</sup>

רוח אשר שם לו למטרה לשפר את הבטיחות של תוכנה ופיתוח בכלל, לחנן לפיתוח מאובטח ובכך להפחית קוד לא מאובטח אשר מוביל לחשיפת ארגונים ואנשים פרטיים למתקפות מטעם גורמים עיינים.

mdi שנה, מפורסם הארגון את 10 החולשות הנפוצות ביותר של אפליקציות רשת בהיבט במתן המקרים בהם נוצאה החולשה בפועל.

אנו נסקור בקצרה את 10 החולשות, אשר אליהן גם התייחסנו בין היתר, בבואהנו לבדוק את מערכת היצויים הטכניונית.

**1. בקרת גישה תקולה** – אפשר גישה למשאים באתר ללא הזרחות ובדיקה הרשות, חוסר במידיניות גישה ברורה לקבצים. לרוב מוביל לדילפת מידע, יכולת עריבת מידע או השחתה.

חולשות נפוצות: יכולת לבצע Directory Traversal, CSRF, עיקוף הזרחות באתר.

**2. חולשה במנגןון הצפנה** – חוסר בהצפנה או בעיה מהותית במנגןון מובילה לכך שמיידע רגיש חשוף לתוכף ומאפשר התחזות, עריבת מידע וכו'...

חולשות נפוצות: שימוש במפתחות שדלו, חוסר שימוש בהצפנה במידע רגיש, מימוש מנגנון הצפנה באופן עצמאי או אלגוריתם הצפנה מיושן שנמצא בו חולשות.

**3. הזרקה** – יכולת הרצת קוד או ביצוע פעולה מחשב כתלות בקלט מהמשתמש, נוצר באשר קלט מהמשתמש לא לבדוק ובנוסף, ישנו מפרש שמאפשר פעולה בהתאם לקלט.

חולשות נפוצות: הזרקת SQL, הזרקת פקודות שרת.

**4. תיכון לא מאובטח** – אי עמידה בדרישות אבטחה, חוסר תכנון לשינויים עתידיים בקוד, מוביל להגדלת משטח התקיפה האפשרי. לדוגמה: אפשר שחזור סיסמה באמצעות שאלה אישית, חוסר חסימת Brute Force וボוטים וכו'...

חולשות נפוצות: הדלפת מידע על המערכת, חוסר באימונות כניסה וגישה למשאים, חולשת העלאת קבצים זדוניים.

**5. הגדרות אבטחה לא מתאימות** – יישום לא נכון של הגדרות אבטחה בסיסיות עלול להוביל ליכולת גישה לא מורשית למשאב ולאפשר התקיפה בשלל איוםים.

---

<sup>1</sup> <https://owasp.org/Top10/>

לדוגמה: גרסאות מיוישנות ופגיעות, השארת הגדרות ברירת מחדל, הדלפת מחסנית הקרייאות וקוד שגיאה, פורטימ פתוחים ללא צורך, חוסר שימוש ב-Headers Headers שנעודו לאבטחה.

**6. רכיבי תוכנה פגיעים ולא מעודכנים** – שימוש במודולים ותלוויות בקוד בספריות לא מאובטחות עם פגיעויות ידועות. ס'API לא בטוחים, קונפיגורציות לא בטוחות לרכיבים שונים בקוד וחוסר עדכוני תוכנה תדיירים, חשופים את התוכנית למתകפות.

חולשות נפוצות: הרצת קוד מרוחק על-ידי ניצול חולשה ברכיב שרך באותו הרשות במו האפליקציה עצמה.

**7. בישולן במנגןן הדיהוי והאימות** – שימוש לא נכון של אימות והזהות עלולים להוביל לחשיפת שמות המשתמשים, סיסמאות, מפתחות ומידע רגיש נספ, ולגרום להתחזות למשתמשים אחרים.

חולשות נפוצות: יכולת מנית משתמשים, הסלמת הרשות, סיסמאות טריוויאליות, Weak Session ID's, Session Fixation

**8. בישולן באימות תוכנה ומידע** – חוסר יכולת לאמת מקורות של ספריות ותלוויות בקוד, עלול להוביל להטמעה של קוד דזוני וניצול על-ידי תוקף. בנוסף, חוסר אימות של סוג המידע, עלול להוביל לפירוש לא נכון שיוביל להרצת קוד.

חולשות והתקפות נפוצות: התקפה על שרשת האספקה, תקיפה דרך העלאת קוד פגיע לספרית קוד פתוח שמתעדכנת אוטומטית, סייראליזציה ודיסיראליזציה לא נכוןה של מידע.

**9. בישולן בניטור ותיעוד** – תיעוד לא מספק או ניטור חלש, בשיתוף עם חוסר במדיניות לתגובה לתרחישים ואיורים חדשים, מאפשר לתוכפים לקבל יכולת התמדה ואחיזה בארגון, התפשטות בתוך הארגון, הרס מידע ויכולת כריית מידע.

**10. זיוף בקשותצד שרת** – מתן שליטה לתוקף להפנות את השרת לבקשת מכתובות שבשליטתו, עלול לחשוף מידע על השרת, לעקוף מנגנוני ההגנה כגון חומות אש ולגרום לניצולו לרעה.

## האיחוד האירופי מאשים את גугл בהפרת החוק להגנת המידע והפרטיות האירופי<sup>2</sup>

לאחר שבית המשפט האוסטרי פסק כי גוגל, דרך המוצר שלה Google Analytics, מפירה את החוק להגנת הפרטיות של תושביה<sup>3</sup> על-ידי איסוף מידע רפואי, שנitinן ליחסו ליישות ספציפית (בגון בתובת AI, היסטוריית גישה, עוגיות וכו') ושליחתו לשרתיה בארה"ב, הגיע הרשות להגנת מידע הצרפית לאוֹתָה המסקנה ופסקה כי פעילותה של Google Analytics אינה חוקית בהתאם לתקנה 44 של החוק להגנת הפרטיות והמידע של האיחוד האירופי.

בין היתר נכתב כי השירות מהווה סיכון למשתמשי האינטרנט בהם מוטמעת המערכת שכן המידע שנאסף אינו נמצא תחת פיקוח הדוק ובנוסף, נגיש לשירותי הבטחון של ממשלה בארה"ב.

מכتبה זו ומשיטוט וקריאה על הנושא באינטרנט, אנו מגיעים למסקנה כי שימוש בכלל של גוגל אינו רצוי במערכת הציונים, שכן, זהה מערכת שנכפה על כל סטודנט להשתמש בה ללא הסכמתו לשילוח המידע עליו לגורם שלישי. אנו נפרט בהמשך מהם ממצאיםינו בנוגע לשימוש במערכת באתר הציונים.



---

<sup>2</sup> <https://iapp.org/news/a/cnil-is-latest-authority-to-rule-google-analytics-violates-gdpr/>

<sup>3</sup> <https://www.dataprotectionreport.com/2022/02/european-rulings-on-the-use-of-google-analytics-and-how-it-may-affect-your-business/>

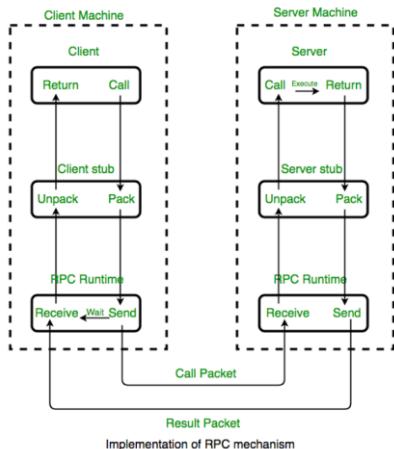
## פרוטוקולים וחולשות מפורסמות:

בהתאם לתוצאות שקיבלנו מתחילה איסוף המידע שביצעו ויפורט בהמשך הדוח, החלטנו להתמקד בטכנולוגיות ובפרוטוקולים הבאים:

- **פרוטוקול FTP** - פרוטוקול תקשורת מבוסס TCP להעברת קבצים בין מחשבים. באמצעות פרוטוקול זה, תוכנת לך **FTP** מתקשרת עם תוכנת שרת **FTP**, לשם לקבלת קובץ מהשרת או הוספת קובץ אליו. לרוב, פרוטוקול זה משתמש בפורט 21 של פרוטוקול TCP. המפרט המקורי של פרוטוקול FTP אינו מתיחס לשאלות של אבטחת מידע, ואין בו כל הצפנה של המידע המועבר.
- **מתקפת SQL Injection** - מתקפה שמוצעת על שירות בסיסי הנתונים המשמשים בטכנולוגיית **SQL** (structured query language) ע"י שימוש בתווים אסורים בתחום השאלתה ששולפת את הנתונים מהשרת, וכן ע"י ניצול היעדר בדיקת קלט כדי לשרר לשאלתה שהאתר מבצע שאילתת נוספת שבה יש לנו שליטה על תנאי השיליפה ועל פרמטרים נוספים.
- **מתקפת כוח גס (brute force)** - מתקפה שמנצלת היעדר מנגןן ויסות ניסיונות התחברות כדי לעبور על כל מרחב האפשרויות הקיימים עבור הסיסמה. ככל שבארגון משתמשים בסיסמאות קצרות יותר וחלשות יותר (אינן מכילות מגוון סוגי של תווים ובאופן שרירותי), כך מתקפה זו הופכת אפקטיבית יותר על אף הפשטות בביוץעה.
- **מתקפת XSS(cross site scripting)** - מתקפות שבהן השירות אינו משתמש בהגנות שתפקידן לוודא שהקלט שמתתקבל אינו מתרגם לקוד JavaScript/HTML דזוני שירות בצד הלקוח. מתחולקות ל-2 סוגים עיקריים:
  - **מתקפת XSS stored** - מתקפה שבה השירות מאפשר שמירה של קוד עליון, כך שכל לקוח שייפנה לדף שבו נמצא הקוד ייריץ אותו בדף שלו.
  - **מתקפת XSS reflected** - מתקפה שבה דף אינטרנט משתמש בקלט שמתתקבל ממשתמש לצורך ייצור "צורך" עמוד HTML דינמי, ולא מודוא שאין קוד דזוני בקלט זה, כך שהאתר עלול להיות פגוע לפרצת XSS דמנית. למתקפה זו מלווה בדרך כלל טכניות של "הנדסה חברתית".
- **פרוטוקול SMB (Server Message Block)** - פרוטוקול תקשורת שעובד בתצורת client-server בו לקוח ה-SMB ניגש דרך פорт TCP 445 ובאמצעות שיטופי SMB אל משאים בגין קבצים, מדפסות שעל שרת ה-SMB. הפרוטוקול מאפשר קיום תקשורת בין מחשבים, כמו גם תקשורת בין תחביבית עם מנגןן הרשות המאפשר את ירשותן. רוב השימוש של SMB הוא במחשבים המרכיבים את מערכת ההפעלה windows microsoft ודרך זו בוצעה בשנת 2017 מתקפת הקופר wannacry שפגעה במאות אלפי מחשבים ברחבי העולם. ביום הגירסאות החדשות יותר נחשבות

למוגנות, בעוד גירסאות ישנות שלא עודכנו חשופות למתקפות.

- **פרוטוקול (II) RPC(Remote Procedure Call)** - טכנולוגיה לתקשורת בין יישומים המאפשרת לתוכנה להפעיל פרצדורה למרחב בתובות אחר (בדרך כלל במחשב אחר) באופן שקויף, בלומר לא צריך בישום פרטני של פרוטוקול התקשורת. באמצעות RPC מתאפשרת



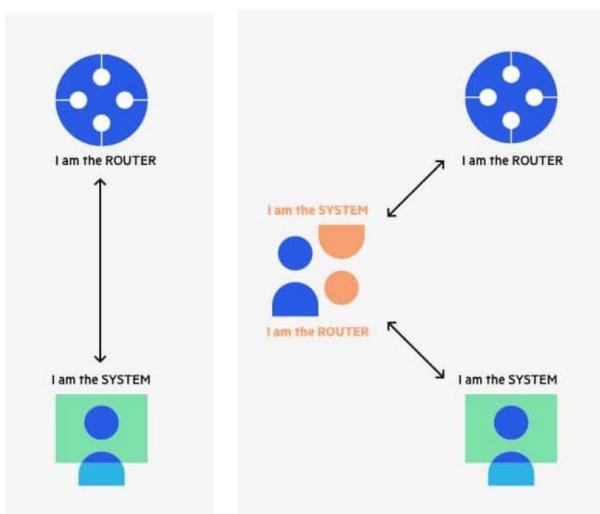
אבסטרקציה בר שnitן לבתוב את אותו הקוד בין אם הוא רץ מקומי על המחשב המריץ אותו או על מחשב מרוחק. באמצעות RPC ניתן למשת תקשורת בתצורת client-server, בר שהליך מפעיל על השרת את הפונקציה הרצiosa תוך העברת הפרמטרים הנדרשים וממתין ממנו לקבלת התשובה. הפרוטוקול מהו אטגר Session לאבטחת מידע שהוא מתחלף מראשו בפורט 135 אך המשך העבודה מתבצע בפורט גבוה (1024-65535) הנקבע דינמית בין השרת לקוח, ולכן stateless firewall לא יעיל.

- **פרוטוקול (III) Microsoft RDP(Remote Desktop Protocol)** - פרוטוקול שפותח ע"י Microsoft ומאפשר קבלת מסך גרפי לחיבור למחשב מרוחק דרך הרשת. הפרוטוקול פועל בדרך כלל מעל פорт TCP/3389 והשימוש בו גבר משמעותית מאז פרוץ מגיפת הקורונה, שכן עובדים רבים עברו לעבוד מביתם והתחרבו ממש למחשב שבמשרד שלהם דרך RDP. מבחינה אבטחתית הבעה העיקרית בכך היא שהחיבור נעשה באמצעות סיסמה התחברות למחשב, שארגונים רבים אינם מקיימים מדיניות שמכריחה שימוש בסיסמות חזקות ולבן תוקף יכול לבצע מתקפת brute force או מתקפת מיליון (שקיים לה איסוף מידע אישי שטוף ביעד התקיפה). כמו כן, תוקפים יכולים להאזין לפורט זהה ולנסות לבצע מתקפת session hijacking / Man

.in the middle

- **מתקפת ARP Poisoning** - פרוטוקול ARP הוא פרוטוקול SMBCAST המריה בין בתובות IP לבתובות או MAC(Media Access Control) של תחנות ברשת. כל תחנה ברשת שומרת טבלה עם ARP Cache כדי לחסוך זמן בשילוח תכמה לעד מוכר, במידה ויעד ההודעה אינו מוכר, מתבצעת שליחת broadcast לרשota LAN שבו נמצא התחנה כדי לנסות לקבל את מהנה אחרת בתובות MAC. פרוטוקול זה אינו תוכנן להיות מאובטח והוא אינו מבצע אימונות לתשובה שהתקבל, ואף אפשר לתחנה לקבל "עדכנים" גם מביי לשלו בקשה ARP, ובכך מתבצע שינוי של ה-

cache. תוקף יכול לנצל זאת כדי לבצע את מתקפת-h Man in the middle**הבא:** הוא ישלח באופן בלתי פ██ק לכל ה-LAN שלו חבילות ARP שאומרות שבתובות MAC של כל בתובות IP ברשת (ובפרט של הנטב) הן בתובות MAC שלו, ובכך כל התעבורה תעבור דרכו והוא יהיה חשוף למידע שאינו מוצפן.



- **שירות NetBIOS(Network Basic Input\Output System)** - זהו שירות רשת שרצה על גבי פורט TCP/139 בשכבה ה-session במודול-h ISO, ומאפשר לאפליקציות שרצות על גבי מחשבים שונים לתקשר זו עם זו דרך רשת LAN (הרשota המקומית). כמו כן NetBIOS יש מגננון המריה בין שמות מחשב ובתובות IP שמהווה תחליף לפוטוקול DNS במצב שבו הוא אינו זמין ושלא הוגדר שרת WINS. ההמרה מתבצעת בין בתובות-h DNS של המחשב ובתובות IP שלו. מבחינה אבטחתית, קיימת בעיות גדולות בשימוש במגנון המריה השמות מכיוון שהשאילתת נשלה בפקודה מעל UDP לכתובות broadcast של LAN, וכן תוקף יכול להסביר לה בראצנו ולמעשה לבצע בקלות מעין ARP Poisoning שטאפער לו להאזין לתעבורה של הקורבן.

- **מתקפת LFI (Local File Inclusion)** - במתתקפה זו התוקף משתמש בפרמטרים שונים בכתובות-h url של האתר על מנת לחשוף קבצים ששמורים על הרשת ולהציג אותם באמצעות הדפסן ואף לעורק קבצים מפורטים שתומכים בכך. היא אפשרית כאשר האתר אינו מבצע אימונות של הפרמטרים שהוא מקבל, ושימוש נפוץ בה הוא directory traversal הקוד של שרת-h web אל תיקייה אחרת. לאחר שהtokf משיג בשלב איסוף

המודיעין מידע על מערכת הפעלה של השרת שעליו האתר רץ, הוא יכול לחשוף קבצים של מערכת הפעלה, כמו למשל passwd/etc ב-xuchs/aetc שambil את שמות המשתמשים שמוגדרים על השרת -wshadow/etc/shadow שambil את ה-hash של הסיסמאות שלהם. לעיתים מתקפה זו יכולה להוביל גם להצלחת ביצוע מתקפת XSS וلمתקפת remote code execution.

## תיאור הפעולות שביצענו

### איסוף מודיעין:

ראשית השתמשנו במקורות גלויים ובכליים ואמצעים אקטיביים לטובת איסוף מידע והבנת משטח התקיפה.

### מציאות Subdomains:

על מנת למצוא את כל ה-Subdomains הרשומים תחת הטכניון, השתמשנו במקורות כגון crt.sh אשר מאפשר חיפוש של סרטייפיקטים שהונפקו לפי ארגון, מתוך מאגר מידע עצום של סרטייפיקטים.

מכיוון שהטכניון משתמש באינומת של הכתובות הנמצאות תחת הדומיין הראשי שלו, ניתן בקלות למצוא את כל ה-SubDomains שלו, וזאת באופן פסיבי מבליל לעורר כל חשד.

רשימה של 500 דומיינים מצורף כקובץ טקסט להתרשומות.

ביצענו גם שימוש במקורות מידע גלויים כמו גוגל כדי למצוא מידע על מערכת הציונים וגילינו על קיומה של המערכת UPGRADE המשמשת את הסגל האקדמי לניהול הסטודנטים והציונים בקורס.

נוסף על ה"סירה" הפסיבית, ביצענו גם סריקה אקטיבית ממוקדת באמצעותה גילינו על קיומו של שרת פיתוח של מערכת UPGRADE, אשר נפרד מערכת ה-Production הגלולה ונמצא באותה הרשת.

כמו כן, גילינו כי קיים מנגנון מושן לצפייה בגילון הציונים בכתבות:

<http://ug3.technion.ac.il/Tadpis.html>

עליו נפרט בהמשך.

## סריקת פורטים פתוחים:

לאחר שמצאנו את ה-sub-domains אשר עשויים להיות רלוונטיים לעובודתנו, פנינו למיפוי הפורטים והשירותים הפתוחים בשרתים של סביבת ה-(o) (132.68.3.58 production) ושל סביבת ה-(o) (132.68.3.36 development).

בעוד במערכת הצוינם לסטודנטים הפורטים היחידים שפתוחים הם 80 ו-443, במערכת UPGRADE ישנו פורטם ושירותים נרחבים יותר שפתוחים ומהווים משטח התקפה:

```
$ nmap -sV 132.68.3.36
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 18:23 EST
Nmap scan report for upgrade-dev.cc.technion.ac.il (132.68.3.36)
Host is up (0.052s latency).
Not shown: 989 filtered tcp ports (no-response), 5 filtered ports (host-unreach)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd
135/tcp   open  msrpc        Microsoft Windows RPC
445/tcp   open  microsoft-ds Microsoft Terminal Services
1433/tcp  open  ms-sql-s    Microsoft SQL Server 2019 15.00.4188
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 69.35 seconds

$ nmap -sV 132.68.3.58
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-18 14:07 EST
Nmap scan report for upgrade-PRO.cc.technion.ac.il (132.68.3.58)
Host is up (0.013s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft IIS ftpt
80/tcp    open  upnp         Microsoft IIS httpd
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  ssl/upnp     Microsoft IIS httpd
445/tcp   open  microsoft-ds Microsoft Terminal Services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 63.96 seconds
```

בתמונה: פורטים פתוחים ושירותים הרצים על-גביים בשרת ה- UPGRADE

## סקירה טכנית של התשתית:

ביצענו ניתוח לאופן ההזהות וההתחברות לאתר הצוינם Grades ולקבלת תדפיס הצוינם באתר sis-Tadpis – פירוט על כך בפרק הממצאים.

את הניתוח ביצענו באמצעות Burp Suite שהנו כלוי עיל המאפשר בין היתר לצפות בכל הפרמטרים העוברים בתקשורת בין הלקוח לשרת וגם באמצעות הכלים למפתחים של דפדפן FireFox אשר מציג באופן נוח את כל המידע העובר בבקשת ובתגובה, כמו גם את העוגיות הנשמרות ומוועברות בבקשתות ותשובות אלו.

Request Body Parameters	
Name	Value
--EVENTTARGET	btnSubmit
--EVENTARGUMENT	
--VIEWSTATE	clirYtlSyLtDCxv0UycPk5p4sN40USNs9lodlTBQQYMB3B...
--VIEWSTATEGENERATOR	C2EE9ABB
--EVENTVALIDATION	GMJUznuzkiPbyAAooFWdQDlfEFtlehcVXxKq6Ncc0y7B3D...
Usertxt	david.deres
Passwordtxt	[REDACTED]
g-recaptcha-response	03AGdBq24Cfq9iTPBEvHSCh4aEXuPq-i6pDgYWNe-AW...

בתמונה: פרמטרים הנשלחים בבקשת ההתחברות לאתר Grades

כמו כן, ניסינו לזהות נקודות תורפה לביצוע הזרקת SQL, למצוא גרסאות מישנות ופגיעה של שירותים הרצים על גבי השירותים השונים ולהבין איך מתבצע אופן ההרשות לצפיה במידע על קורסים מסוימים (מצאים בהמשך).

```
(kali㉿kali)-[~]
└─$ nmap -sV --script=banner 132.68.239.19 -p 80
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-22 06:12 EST
Nmap scan report for grades.technion.ac.il (132.68.239.19)
Host is up (0.096s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.15 seconds

PORT      STATE SERVICE VERSION
443/tcp   open  ssl/http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-trane-info: Problem with XML parsing of /evox/about
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

בתרמונה: קיבלת מידע על שירות ה-HTTP ו-HTTPS של שרת Grades

חדר בדיחה	מספר	שם פרטי	שם משפחה	שם שמי	שם ארכון	תאריך בדיחה	שם מבחן				
(805) לילן	3.11	17:30	02/01/2022	יום ראשון	Midterm 1						
ענין לא הוקצת חדרים לבחינה	3.40		31/01/2022	יום שני	Exam A						
ענין לא הוקצת חדרים לבחינה	2.40		31/01/2022	יום שני	Exam A						
ענין לא הוקצת חדרים לבחינה	3.553		13/02/2022	יום ראשון	Exam A						
ענין לא הוקצת חדרים לבחינה	3.61		21/02/2022	יום שני	Exam A						
	3.67		27/02/2022	יום ראשון	Exam B						
	3.576		08/03/2022	יום שלישי	Exam B						
	2.76		08/03/2022	יום שלישי	Exam B						

בתרמונה: דוגמא לשימוש בכלל אוטומטי אשר מותן סקירה של הטכנולוגיות והספריות בהן נעשה שימוש באתר

בתרמונה: הודעת שגיאה המוביילה לחסיפה של גרסה .NET באמצעות פותחן האתר

```
(kali㉿kali)-[~/Downloads]
└─$ nmap --script=smb2-security-mode.nse 132.68.3.58
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-23 08:19 EDT
Nmap scan report for Upgrade-PRD.cc.technion.ac.il (132.68.3.58)
Host is up (0.0073s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
585/tcp   open  ncacn-tcp:[LRPC-88638e4d722546fe0e]
5855/tcp  open  ncacn-rpc:[OLEA58835101C177153CCBDFC948406]
5856/tcp  open  ncalrpc:[OLEA58835101C177153CCBDFC948406]
Host script results:
| smb2-security-mode:
|   3.1.1:
|     Message signing enabled but not required
5855/tcp  open  ncacn-rpc:[OLEA58835101C177153CCBDFC948406]
Nmap done: 1 IP address (1 host up) scanned in 51.24 seconds
```

בתמונה: דוגמא לבדיקה של גרסה SMB על שרת UPGRADE לבודיקת פגיעות ידועה בפרוטוקול

```
(kali㉿kali)-[~]
└─$ nmap --script "rdp-enum-encryption or rdp-vuln-ms12-020 or rdp-ntlm-info" -p 3389 -T4 132.68.3.36
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-15 11:07 EDT
Nmap scan report for upgrade-dev.cc.technion.ac.il (132.68.3.36)
Host is up (0.070s latency).

PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
  rdp-enum-encryption:
    Security layer
      CredSSP (NLA): SUCCESS
      CredSSP with Early User Auth: SUCCESS
      RDSTLS: SUCCESS
      SSL: SUCCESS
  - RDP Protocol Version: RDP 10.6 server
  rdp-ntlm-info:
    Target_Name: CC-ROOT
    NetBIOS_Domain_Name: CC-ROOT
    NetBIOS_Computer_Name: UPGRADE-DEV
    DNS_Domain_Name: cc.technion.ac.il
    DNS_Computer_Name: Upgrade-Dev.cc.technion.ac.il
    DNS_Tree_Name: cc.technion.ac.il
    Product_Version: 10.0.17763
    System_Time: 2022-03-15T15:07:04+00:00
Nmap done: 1 IP address (1 host up) scanned in 3.11 seconds
```

בתמונה: דוגמא לבדיקה של גרסה RDP על שרת UPGRADE לבודיקת פגיעות ידועה בפרוטוקול

## פעולות אקטיביות:

### נסיין עקיפת מנגןן ההזדהות באתר Grades

הזהדות באתר **Grades** מתבצעת באמצעות אמצעות **.ASP.NET Forms-Based Authentication** והזהדות באתר היא כדרלהן:

המשתמש מכניס שם משתמש וסיסמה טכניוניים. עם הלחיצה על כפתור ההתחברות, נשלחת בקשה POST על-גבי HTTP לשרת, עם הפרמטרים הבאים:

Request Body Parameters	
Name	Value
--EVENTTARGET	btnSubmit
--EVENTARGUMENT	
--VIEWSTATE	clirYtlSyLtDCxv0UycPk5p4sN40USNs9lodlTBQQYMB3B...
--VIEWSTATEGENERATOR	C2EE9ABB
--EVENTVALIDATION	GMJUznuzkiPbyAAooFWdQDlfEFtlehcVXxKq6Ncc0y7B3D...
Usertxt	david.deres
Passwordtxt	[REDACTED]
g-recaptcha-response	03AGdBq24Cfq9iTpbEvHSCh4aEXuPq-i6pDgYWNe-AW...

VIEWSTATE - מזהה אשר נועד לתת הקשר למשתמש, מאפשר לאתר להיות Stateful ולשמור על עקבות בשינויים ומידע ש摹צג למשתמש בדף שלו.

ViewState - VIEWSTATEGENERATOR

Usertxt - שם המשתמש

Passwordtxt - סיסמא

g-recaptcha-response - מענה אוטומטי על Google ReCAPTCHA, מנגן למניעת בוטים

כמו כן, נשלחות עם הבקשה העוגיות הבאות:

Request Cookies	
Name	Value
_ga	GA1.3.164894668.164...
TechnionGrades	szxzyjzclibpb1wfqey4va...

\_ga : עוגיות המשמשות את Google Analytics לזהויו המשתמש - פירוט בחלק של הפרט הפרסיות.

TechnionGrades : עוגיה המציינת את ה-session ומקושרת למשתמש לאחר ההזדהות מוצלחת על-מנת לגשת למידע על קורסים ולקבל את הציונים הרלוונטיים.

בתגובה להתחברות מוצלחת נשלחת עוגית ASPXFORMSAUTH מוצפנת אשר מעידה על בר שזההות של המשתמש הספציפי הייתה מוצלחת.

## Response

Pretty Raw Hex Render ⌂ ⌄ ⌅

```
1 | HTTP/2 302 Found
2 | Cache-Control: private
3 | Content-Type: text/html; charset=us-ascii
4 | Location: /index.aspx
5 | Set-Cookie: .Grades ASPXFORMSAUTH=
49171ABC65FC8B35A6D4F51557F8D6A75BF41C3794FD815F58758BF839DEB5CEED70E173
2F27C12C4F8384976D4BDCFADDAEDEE4753A6DDDC8D2F08A5ED822DA0A26C1BE47EAB429
0A7600CF966609FC61F2F8D3C01B19B2860C2957DB71368ACF77191320BE0090BE58DF76
7C5AD489F3638E7E64554E461B55A18CA4ECC53E; path=/; secure; HttpOnly;
```

זהו עוגה שמצוורפת לכל בקשה מכאן ואילך ומעידה על כך שהמשתמש אומת, יש לה זמן מוקצב (לא ניתנת לשימוש חודר).

הניסיונות שביצענו:

שימוש חוזר בעוגיה: לאחר ב-5 דקות העוגיה לא תקפה להזדהות

גישה ושירה לדפים ידועים או ע"י אינומרכיה: עם כל בקשה נשלחת העוגיה גישה ושירת הדפים ייחד עם עוגיות האימות. הגישה ניתנת רק לדפים שהמשתמש מורשה TechnionGrades לצפות בהם:

The screenshot shows a browser's developer tools Network tab with several requests listed. The first request is a GET to `/content.aspx?cID=52864`. The response for this request includes a `Set-Cookie` header for the `.Grades` cookie, which contains a long alphanumeric string. The Inspector tab shows the details of this cookie, including its name, value, and expiration date.

יחד עם זאת, שמננו לב שנשלחות עוגיות רבות המשויכות לגולג'ל יחד עם בקשה לקבלת מידע, מה שעורר את חשדנו ועל כך נפרט בהמשך.

חיפוש חולשה בהצפנה: מצאנו דוגמא לאופן בו צד השרת מאמת ומצפין את המידע<sup>4</sup>, בקצרה: הפרמטרים של המשתמש בעברית ולידציה באמצעות השוואת הגיבוב שלו, יחד עם שדות נוספים כמו תאריך נוכחי ותוקף העוגיה מוצפנים באמצעות אלגוריתם הצפנה ידוע עם שימוש ב-7!, שיטת ההצפנה, כמו גם הפרמטרים הנוספים נקבעים על ידי מתכון

<sup>4</sup> <https://gist.github.com/amanda-mitchell/5350992>

האתר באמצעות מנגנון ניהול של ASP.NET (לרוב נבחר אלגוריתם AES). יחד עם ההגדרות, נמצא מפתח הצפנה בקובץ `web.config` אשר אינו נגיש.

חולשה נפוצה היא שימוש במפתחות ברירת מחדל, או מפתחות הצפנה שמשמעותם באינטרנט, כאשר מנהלי אתרים נתקלים בעיה במנגנון ומעתיקים את המפתח שמציעים להם כדוגמה (קיימים צהה אפילו באתר של מיקרוסופט<sup>5</sup>)

The screenshot shows a Stack Overflow question page. The URL in the address bar is <https://stackoverflow.com/questions/1360078/asp-net-mvc-validation-of-viewstate-mac-failed>. The question title is "Under the covers, the MVC AntiForgeryToken attribute uses the machinekey for encryption. If you don't specify a machinekey in the web.config (see [here](#)), one is automatically generated for you by ASP.NET ([full description](#)).". The question has 32 answers. One answer, by user 'Dunc', provides XML code for the web.config file:

```
<configuration>
  <system.web>
    <machineKey
      validationKey="21F090935F6E49C2C797F69BAAAD8402ABD2EE0B667A8B44EA7DD4374267A75D74"
      decryptionKey="ABAA84D7EC4BB56D75D217CECFB9628809BDB8BF91CFC64568A145BE59719F"
      validation="SHA1"
      decryption="AES"
    />
```

The answer was edited on Oct 16 '09 at 11:35 and answered on Oct 16 '09 at 10:07 by user 'Dunc'. It has 13.7k views, 4 votes, 56 comments, and 82 answers. A comment below the answer states: "I am still getting the error even if I enter the machineKey like this. Could it be that the machine config on the server (I have not access to this) is not configured correctly? – jesperlind Nov 12 '09 at 1:54".

פרויקט BlackList3r<sup>6</sup> הינו פרויקט במסגרתו נאפסו מעל 3000 מפתחות הצפנה שנמצאו בסקרים ברחבי הרשת כחלק מהגדרת שרת ASP.NET. חלק מהפרויקט נכתב קוד אשר מאפשר לבדוק בהינתן טקסט מסוון, האם הוא הוצפן באמצעות אחד ממפתחות אלו, ע"י הרצת כל אלגוריטמי הצפנה והפענוח האפשריים ב-.NET.

במקרה שלנו, לא נמצא כי נעשה שימוש במפתח חלש/מומחזן:

<sup>5</sup> <https://docs.microsoft.com/en-us/iis/troubleshoot/security-issues/troubleshooting-forms-authentication>

<sup>6</sup> <https://notosecure.com/project-blacklist3r>

```
D:\Semester 7\InfoSec Project\AspNetWrapper>AspDotNetWrapper.exe --keypath MachineKeys.txt --encrypteddata 6F07B56F4B87512392CAFEB89BCD56F1D99A2B00CD7C053B9008AE71FD84FD7F0F900623A96f4B4B036A4FC487F999
12F4122C7D0C33F3260F195FCF0F7B63DA67B01C87C2381057E0273BA0780091943E962132CE62016620B064545D4A1568D1EB055023451E3F17B8A504EC099A10202C0AE91715665C017A6999 - decrypt --purpose=aspauth

Decryption process start!!
Processing machinekeys TripleDES,HMACSHA512: 3571/3571.....
Keys not found!!
```

## חולשה באימות המידע :(Serialization and Deserialization)

חולשה נפוצה שקיימת בפלטפורמת ASP.NET הנה הזרקה של Payload ידוע מראש דרך ViewState, אך שבאמצעות פירוש לא נכון של ה-Payload, ניתן להגיע להרצת קוד מרוחק על המכוונה<sup>7</sup>.

באtor Grades, חולשה זו לא באה לידי ביטוי ביום ש-ViewState עובר הצפנה ופענוח על ידי השירות, אך ללא מפתח ההצפנה, לא ניתן לשלוח את ה-Payload הרצוי.

בנסיכוןינו "לשחק" עם ה-ViewState, הצלחנו להגעה להדפסה של ה-

The screenshot shows a Fiddler session. The Request tab displays a POST request to `/Login.aspx` with various headers (Content-Type, User-Agent, Accept, etc.) and a body containing ViewState data. The Response tab shows an error message: ".Server Error in '/' Application" and ".The state information is invalid for this page and might be corrupted". Below the message is a stack trace:

```

    .Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.
    .Exception Details: System.Web.HttpException: The state information is invalid for this page and might be corrupted
    .Source Error
    :The source code that generated this unhandled exception can only be shown when compiled in debug mode. To enable this, please follow one of the below steps, then request the URL:
    :Add a "Debug=true" directive at the top of the file that generated the error. Example .i
    :<%@ Page Language="C#" Debug="true" %>
    :or
    :Add the following section to the configuration file of your application (2
    <configuration>
        <system.web>
            <compilation debug="true"/>
        </system.web>
    </configuration>

    .Note that this second technique will cause all files within a given application to be compiled in debug mode. The first technique will cause only that particular file to be compiled in debug mode.
    .Important: Running applications in debug mode does incur a memory/performance overhead. You should make sure that an application has debugging disabled before deploying into production scenario

```

The stack trace points to the method `System.Web.Util.DeserializeWithAssert(IStateFormatter2 formatter, String serializedState, Purpose purpose) +65`.

<sup>7</sup> <https://soroush.secproject.com/blog/2019/04/exploiting-deserialisation-in-asp-net-via-viewstate/>

```

[FormatException: Invalid length for a Base-64 char array or string.]
  System.Convert.FromBase64_Decode(Char* startInputPtr, Int32 inputLength, Byte* startDestPtr, Int32 destLength) +14218845
  System.Convert.FromBase64CharPtr(Char* inputPtr, Int32 inputLength) +131
  System.Convert.FromBase64String(String s) +50
  System.Web.UI.ObjectStateFormatter.Deserialize(String inputString, Purpose purpose) +86
  System.Web.UI.Util.DeserializeWithAssert(IStateFormatter2 formatter, String serializedState, Purpose purpose) +65
  System.Web.UI.HiddenFieldPageStatePersister.Load() +179

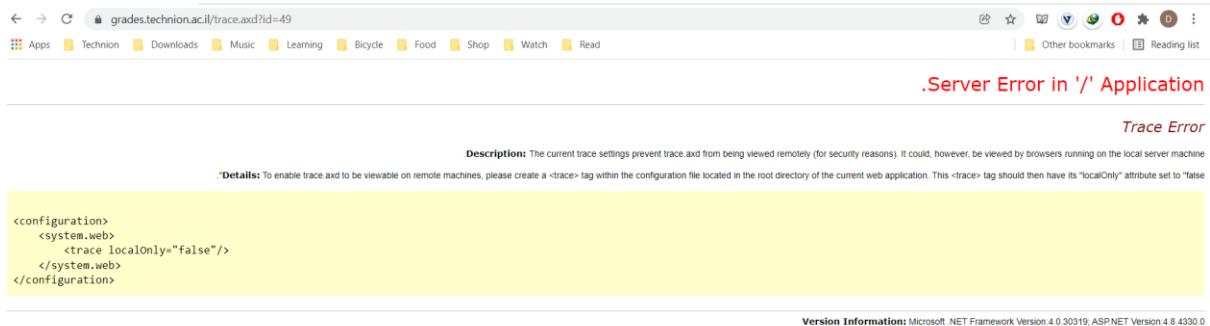
[ViewStateException: Invalid viewstate.
  Client IP: 46.121.222.156
  Port: 51485
  Referer: https://grades.technion.ac.il/login.aspx
  Path: /login.aspx
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
  ViewState: AAA]

[HttpException (0x80004005): The state information is invalid for this page and might be corrupted.]
  System.Web.UI.ViewStateException.ThrowError(Exception inner, String persistedState, String errorPageMessage, Boolean macValidationError) +161
  System.Web.UI.HiddenFieldPageStatePersister.Load() +332
  System.Web.UI.Page.LoadPageStateFromPersistenceMedium() +377
  System.Web.UI.Page.LoadAllState() +46
  System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +9318
  System.Web.UI.Page.ProcessRequest(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +355
  System.Web.UI.Page.ProcessRequest() +79
  System.Web.UI.Page.ProcessRequest(HttpContext context) +74
  ASP.login.aspx.ProcessRequest(HttpContext context) +46
  System.Web.CallHandlerExecutionStep.System.Web.HttpApplication.IExecutionStep.Execute() +542
  System.Web.HttpApplication.ExecuteStepImpl(IExecutionStep step) +75
  System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchronously) +93

```

בתמונה: ניתן לראות במרכז היישוי שנשלח בבקשת מודפס בחלק מה- Response

**על אף שמנגנון זה מבוטל (מכיוון שהוא אופציוני לחסוף דיבוג שלולה להיות חשופה עקב מיסקונפיגורציה של השרת):**



## נסו לגשת לדף הראשי במשחק הציונים של הסגל UPGRADE ללא הזרות, עם עוגיות ASPXFORMSAUTH:

לא אפשר גישה, נראה ישם מאפיינים ייחודיים וטוניים לעוגיות האימות על פני שני האתרים

## בדיקות יכולת הרצת XSS באתר Grades

מכיוון שאין באתר Grades שדות למילוי ע"י המשתמש אלא רק מידע ל视象, ניצלו את העבודה שבהזרעת השגיה מרונדר דף HTML עם ה- ViewState שהקלנו, כדי לנסות להבין האם מבוצע סינוון של תוכן המגיע מצד הלוק והאם מבוצעת סנייטיזה לפלט שנשלח בתגובה מהשרת.

#### המצאים: מבוצע סיכון לבקשת:

```
[FormatException: The input is not a valid Base-64 string as it contains a non-base 64 character, more than two padding characters, or an illegal character among the padding characters. ]
System.Convert.FromBase64Decode(Char* startInputPtr, Int32 inputLength, Byte* startDestPtr, Int32 destLength) +14218401
System.Convert.FromBase48CharTrg(Char* inputPtr, Int32 inputLength) +131
System.Convert.FromBase48String(String s) +50
System.Web.UI.ObjectStateFormatter.Deserialize(String inputString, Purpose purpose) +86
System.Web.UI.Util.DeserializeWithAssert(IStateFormatter2 formatter, String serializedState, Purpose purpose) +65
System.Web.UI.HiddenFieldPageStatePersister.Load() +179

[ViewStateException: Invalid viewstate.
Client IP: 46.121.222.156
Port: 61989
Referer: https://grades.technion.ac.il/login.aspx
Path: /login.aspx
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36
ViewState: {u003c/div{u003e{u003cscript{u003e{u003ea{u0031{u003c/u003e{script{u003e{u003cdiv{u003e}
```

בתמונה: ניתן לראות שמחוז פלט שעובר "ציטוט", הכולמר סיכון בפועל של הבקשה

ובנוסף, מבוצעת סניתציה לתגובה:

בתרמונה: ניתן לראות בקשה הכוללת את התווים <-> בקידוד utf16be אשר מתורגם ל-  
gt;&-lt;

## יבולת Enumeracion

האתר חושף חולשת מניה של המשתמשים הרשומים, על-ידי כך שמווחר such user so עבור משתמש שאינו רשום במערכת. ניתן לבצע אוטומציה של החולשה וליצור רשימה של משתמשים קיימים לפי הפלט המוחזר.

פקום גוף בו מזאך חולשה זו הוא במנגנון שחזור הסיסמה ששיר למייקרוסופט.

**Grading System**

User: daadadaczxcdsf  
Password: Password

Log in →

protected by reCAPTCHA  
Privacy - Terms

**no such user**  
for Explanation of authentication [Click here](#)

Suggestions and Comment Wall : [Personal.Portal@technion.ac.il](mailto:Personal.Portal@technion.ac.il)

**חזרה לחשבון שלך**

מי אתה?

דואר אלקטרוני או שם משתמש: \*

yoyo@campus.technion.ac.il

דגם: user@contoso.com OR user@contoso.onmicrosoft.com

דואר אלקטרוני או שם המשתמש שהזנת כראוי את הדואר האלקטרוני או את שם המשתמש שלך.

חוץ את התווים בתמונה או את המילים בשמעו.\*

המשך      ביטול

## יבולת BruteForce באתר Tadpis

באטר שבסתוות: <http://ug3.technion.ac.il/Tadpis.html> ניתן לצפות בתדפיס הציונים של הסטודנט. הרתחברות לאתר זה נעשית ע"י הזנת תעוזת הזרות והסיסמה הראשונית של הסטודנט לימודי הסמבה, שמכילה 8 ספרות בדוק. האתר אינו מאפשר הזנת תווים שאינם ספרות לטור שדה הסיסמה ומודיעו למשתמש על כך, ואורך הקלט המאפשר ת"ז של סטודנט, מרחיב האפשרויות לסיסמה הוא 10 בחזקת 8. באתר לא קיים מנגנון שיחסם גישה לאחר מספר רב של ניסיונות תוך זמן קצר (כמו מנגנון Captcha שקיים באתר Grades), ובפיו שניתן לראות בצלומי המסך הבאים, כלים אוטומטיים שמבצעים מתקפת מילון יכולים לגלוות את הסיסמה תוך זמן לא ארוך (היות והסיסמה קבועה אינה משתנה כלל). הדבר עשוי להוות פגיעה בפרטיות הסטודנט, בנוסף גילוין זה הינו מפורט יותר מ"תעודת הציונים" ומציג את כל הציונים שהסטודנט קיבל במהלך כל לימודי האקדמיים, גישה אליו עשויה להיות חיונית עבור בעלי עניין כגון חברות מסחריות שלווהו הסטודנט מתראיין.

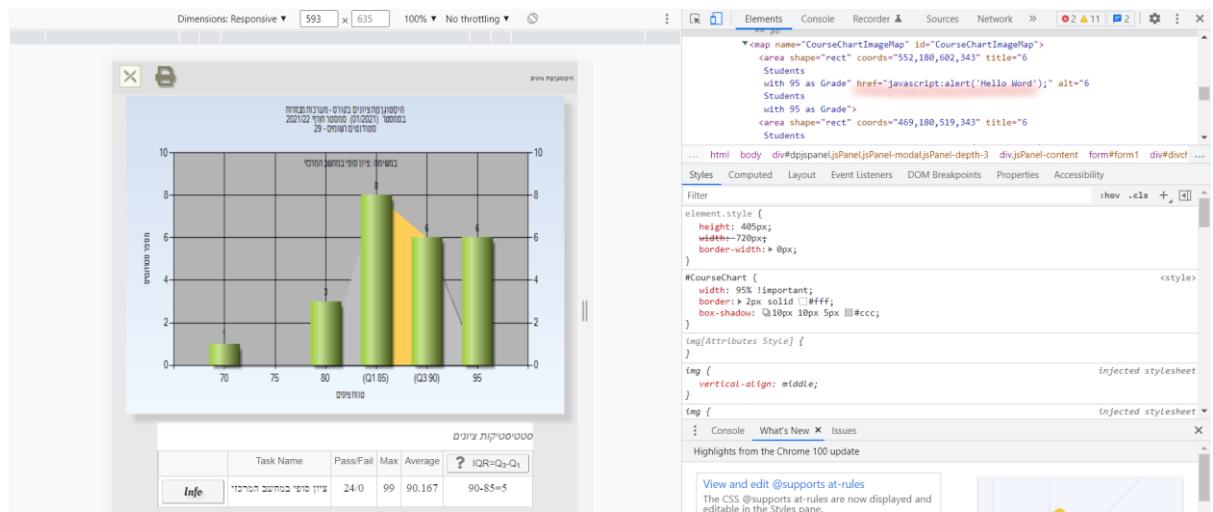
```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-17 05:47:37
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100000000 login tries (1:1/g:100000000), -6250000 tries per task
[DATA] attacking http-post-form://ug3.technion.ac.il:80/Tadpis.html:function-signinuserId="USER"password="PASS":F=CICS Web Interface signon unsuccessful
[0][http-post-form host: ug3.technion.ac.il login: password: 00000003
[0][http-post-form host: ug3.technion.ac.il login: password: 00000004
[0][http-post-form host: ug3.technion.ac.il login: password: 00000005
[0][http-post-form host: ug3.technion.ac.il login: password: 00000006
[0][http-post-form host: ug3.technion.ac.il login: password: 00000007
[0][http-post-form host: ug3.technion.ac.il login: password: 00000008
[0][http-post-form host: ug3.technion.ac.il login: password: 00000009
[0][http-post-form host: ug3.technion.ac.il login: password: 00000010
[0][http-post-form host: ug3.technion.ac.il login: password: 00000011
[0][http-post-form host: ug3.technion.ac.il login: password: 00000012
[0][http-post-form host: ug3.technion.ac.il login: password: 00000013
[0][http-post-form host: ug3.technion.ac.il login: password: 00000014
[0][http-post-form host: ug3.technion.ac.il login: password: 00000015
[0][http-post-form host: ug3.technion.ac.il login: password: 00000016
[0][http-post-form host: ug3.technion.ac.il login: password: 00000017
[0][http-post-form host: ug3.technion.ac.il login: password: 00000018
[0][http-post-form host: ug3.technion.ac.il login: password: 00000019
[0][http-post-form host: ug3.technion.ac.il login: password: 00000020
[0][http-post-form host: ug3.technion.ac.il login: password: 00000021
[0][http-post-form host: ug3.technion.ac.il login: password: 00000022
[0][http-post-form host: ug3.technion.ac.il login: password: 00000023
[0][http-post-form host: ug3.technion.ac.il login: password: 00000024
[0][http-post-form host: ug3.technion.ac.il login: password: 00000025
[0][http-post-form host: ug3.technion.ac.il login: password: 00000026
[0][http-post-form host: ug3.technion.ac.il login: password: 00000027
[0][http-post-form host: ug3.technion.ac.il login: password: 00000028
[0][http-post-form host: ug3.technion.ac.il login: password: 00000029
[0][http-post-form host: ug3.technion.ac.il login: password: 00000030
[0][http-post-form host: ug3.technion.ac.il login: password: 00000031
[0][http-post-form host: ug3.technion.ac.il login: password: 00000032
[0][http-post-form host: ug3.technion.ac.il login: password: 00000033
[0][http-post-form host: ug3.technion.ac.il login: password: 00000034
[0][http-post-form host: ug3.technion.ac.il login: password: 00000035
[0][http-post-form host: ug3.technion.ac.il login: password: 00000036
[0][http-post-form host: ug3.technion.ac.il login: password: 00000037
[0][http-post-form host: ug3.technion.ac.il login: password: 00000038
[0][http-post-form host: ug3.technion.ac.il login: password: 00000039
[0][http-post-form host: ug3.technion.ac.il login: password: 00000040
[0][http-post-form host: ug3.technion.ac.il login: password: 00000041
[0][http-post-form host: ug3.technion.ac.il login: password: 00000042
[0][http-post-form host: ug3.technion.ac.il login: password: 00000043
[0][http-post-form host: ug3.technion.ac.il login: password: 00000044
[0][http-post-form host: ug3.technion.ac.il login: password: 00000045
[0][http-post-form host: ug3.technion.ac.il login: password: 00000046
[0][http-post-form host: ug3.technion.ac.il login: password: 00000047
[0][http-post-form host: ug3.technion.ac.il login: password: 00000048
[0][http-post-form host: ug3.technion.ac.il login: password: 00000049
[0][http-post-form host: ug3.technion.ac.il login: password: 00000050
[0][http-post-form host: ug3.technion.ac.il login: password: 00000051
[0][http-post-form host: ug3.technion.ac.il login: password: 00000052
[0][http-post-form host: ug3.technion.ac.il login: password: 00000053
[0][http-post-form host: ug3.technion.ac.il login: password: 00000054
[0][http-post-form host: ug3.technion.ac.il login: password: 00000055
[0][http-post-form host: ug3.technion.ac.il login: password: 00000056
[0][http-post-form host: ug3.technion.ac.il login: password: 00000057
[0][http-post-form host: ug3.technion.ac.il login: password: 00000058
[0][http-post-form host: ug3.technion.ac.il login: password: 00000059
[0][http-post-form host: ug3.technion.ac.il login: password: 00000060
[0][http-post-form host: ug3.technion.ac.il login: password: 00000061
[0][http-post-form host: ug3.technion.ac.il login: password: 00000062
[0][http-post-form host: ug3.technion.ac.il login: password: 00000063
[0][http-post-form host: ug3.technion.ac.il login: password: 00000064
[0][http-post-form host: ug3.technion.ac.il login: password: 00000065
[0][http-post-form host: ug3.technion.ac.il login: password: 00000066
[0][http-post-form host: ug3.technion.ac.il login: password: 00000067
[0][http-post-form host: ug3.technion.ac.il login: password: 00000068
[0][http-post-form host: ug3.technion.ac.il login: password: 00000069
[0][http-post-form host: ug3.technion.ac.il login: password: 00000070
[0][http-post-form host: ug3.technion.ac.il login: password: 00000071
[0][http-post-form host: ug3.technion.ac.il login: password: 00000072
[0][http-post-form host: ug3.technion.ac.il login: password: 00000073
[0][http-post-form host: ug3.technion.ac.il login: password: 00000074
[0][http-post-form host: ug3.technion.ac.il login: password: 00000075
[0][http-post-form host: ug3.technion.ac.il login: password: 00000076
[0][http-post-form host: ug3.technion.ac.il login: password: 00000077
[0][http-post-form host: ug3.technion.ac.il login: password: 00000078
[0][http-post-form host: ug3.technion.ac.il login: password: 00000079
[0][http-post-form host: ug3.technion.ac.il login: password: 00000080
[0][http-post-form host: ug3.technion.ac.il login: password: 00000081
[0][http-post-form host: ug3.technion.ac.il login: password: 00000082
[0][http-post-form host: ug3.technion.ac.il login: password: 00000083
[0][http-post-form host: ug3.technion.ac.il login: password: 00000084
[0][http-post-form host: ug3.technion.ac.il login: password: 00000085
[0][http-post-form host: ug3.technion.ac.il login: password: 00000086
[0][http-post-form host: ug3.technion.ac.il login: password: 00000087
[0][http-post-form host: ug3.technion.ac.il login: password: 00000088
[0][http-post-form host: ug3.technion.ac.il login: password: 00000089
[0][http-post-form host: ug3.technion.ac.il login: password: 00000090
[0][http-post-form host: ug3.technion.ac.il login: password: 00000091
[0][http-post-form host: ug3.technion.ac.il login: password: 00000092
[0][http-post-form host: ug3.technion.ac.il login: password: 00000093
[0][http-post-form host: ug3.technion.ac.il login: password: 00000094
[0][http-post-form host: ug3.technion.ac.il login: password: 00000095
[0][http-post-form host: ug3.technion.ac.il login: password: 00000096
[0][http-post-form host: ug3.technion.ac.il login: password: 00000097
[0][http-post-form host: ug3.technion.ac.il login: password: 00000098
[0][http-post-form host: ug3.technion.ac.il login: password: 00000099
[0][http-post-form host: ug3.technion.ac.il login: password: 000000100
```

2. Intruder attack of techmvs.technion.ac.il - Temporary attack - Not saved to project file						
Attack	Save	Columns	Results	Target	Positions	Payloads
Results	Target	Positions	Payloads	Resource Pool	Options	
Filter: Showing all items						
Request	Payload	Status	Error	Timeout	Length	Comment
73	00999973	200			5121	
74	00999974	200			5121	
75	00999975	200			5121	
76	00999976	200			5121	
77	00999977	200			5121	
78	00999978	200			5121	
79	00999979	200			5121	
80	00999980	200			5121	
81	00999981	200			5121	
82	00999982	200			5121	
83	00999983	200			5121	
84	00999984	200			5121	
85	00999985	200			5121	
86	00999986	200			5121	
87	00999987	200			5121	
88	00999988	200			5121	
89	00999989	200			5121	
90	00999990	200			5121	
91	00999991	200			5121	
92	00999992	200			5121	
93	00999993	200			5121	
94	00999994	200			5121	
95	00999995	200			5121	
96	00999996	200			5121	
97	00999997	200			5121	
98	00999998	200			5121	
99	00999999	200			5121	
100	009999999	302			964	

## מעבר על קוד SJ למציאת חולשות:

חלק מנשיאותינו כללו מעבר על הקוד שנטען בדףן בחלק מהגילהה באתר.

אמנם לא מצאנו חולשה ממשית הנחנית לניצול על-ידי תוקף, אך גילינו כי קיים Stored XSS בקוד, אשר נתען עם בקשת צפיה בהיסטוגרמות של כלקורס.



Screenshot of Burp Suite showing a list of captured requests and their details. The list includes columns for #, Host, Method, URL, Params, Edited, Status, Length, MIME type, Extension, Title, Comment, TLS, and IP. A specific request at index 353 is highlighted, showing a GET request to /chart.aspx?ID=10000. The response content is displayed in the 'Response' tab, showing HTML code for a chart. The 'Inspector' tab shows request attributes, query parameters, and cookies for this specific request.

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP
169	https://fonts.gstatic.com	GET	/ls/robot/v18/KFOICnqEu92Fr1MmEU...			200	16495	woff2		מודיע על משימות למק...	✓	142.250.185.67	
170	https://fonts.gstatic.com	GET	/ls/robot/v18/KFOICnqEu92Fr1MmU...			200	16287	woff2		בקורס - מסדי נתונים ב...	✓	142.250.185.67	
89	https://fonts.gstatic.com	GET	/ls/leescrpt/v14/raxHieDtM0e0lCs...			200	13399	woff2		מודיע על משימות למק...	✓	142.250.185.67	
51	https://fonts.gstatic.com	GET	/ls/robot/v18/KFOICnqEu92Fr1MmEU...			200	16495	woff2		מודיע על משימות למק...	✓	142.250.186.35	
50	https://fonts.gstatic.com	GET	/ls/robot/v18/KFOICnqEu92Fr1MmU...			200	16287	woff2		מודיע על משימות למק...	✓	142.250.186.35	
361	https://grades.technion.ac.il	GET	/content.aspx?ID=52792	✓		200	30201	HTML	aspx	מודיע על משימות למק...	✓	132.68.239.19	
353	https://grades.technion.ac.il	GET	/chart.aspx?ID=10000	✓		200	7975	HTML	aspx	מודיע על משימות למק...	✓	132.68.239.19	
329	https://grades.technion.ac.il	GET	/js/content-1.0.0.js			200	2187	script	js	מודיע על משימות למק...	✓	132.68.239.19	
328	https://grades.technion.ac.il	GET	/js/Scan-3.0.js			200	7534	script	js	מודיע על משימות למק...	✓	132.68.239.19	
338	https://grades.technion.ac.il	GET	/js/CourseStatistics-4.0.4.js			200	14149	script	js	מודיע על משימות למק...	✓	132.68.239.19	
317	https://grades.technion.ac.il	GET	/content.aspx?ID=52864	✓		200	25571	HTML	aspx	מודיע על משימות למק...	✓	132.68.239.19	
308	https://grades.technion.ac.il	GET	/js/Index-2.0.7.js			200	8212	script	js	מודיע על משימות למק...	✓	132.68.239.19	
291	https://grades.technion.ac.il	GET	/Index.aspx			200	50452	HTML	aspx	מודיע על משימות למק...	✓	132.68.239.19	
289	https://grades.technion.ac.il	GET	/Index.aspx			200	50452	HTML	aspx	מודיע על משימות למק...	✓	132.68.239.19	

לא ניתן לדעת מהיבין הגיעו שורות קוד אלו לשרת, אך זה בהחלט יכול להעיד על יכולת הרצת קוד על-ידי גורם עיוון ונדרש לבדוק עם מתחזקי האתר האם הם מודעים לכך. (אפקטiva נוספת נספהת היא שמדובר בהלצה מצד כתבי הקוד)

ממצא נוסף ומשמעותי הוא המעורבות שיש לגוגל באתר הציוןים, או ליתר דיוק, שליחת המידע לשרת גולן בשיתוף פעולה עם מתכנתיו באתר.

כפי שציינו בסקר הספרות, גולן אינו מזוהה עם שמירה על פרטיות ואף הפר לא פעם חוקים של מדיניות ערביות בכל הנוגע להגנה על פרטיות ושמירה על מידע אישי.

מעבר על הקוד, כמו גם ניתוח אופן התקשורת והאימוטים באתר, גילינו כי לאורך כל הגלישה נוצרות וൺשות עוגיות הקשורות את המשתמש עם שירותים גולן, ביניהם Google Analytics, Google Tags and Google Translate

להלן מספר צילומי מסך המדגימים את היקף המעורבותה זו בקוד והן בכמות העוגיות והפרמטרים המשותפים עם גולן:

## Tag Manager overview

Google Tag Manager is a [tag management system](#) (TMS) that allows you to quickly and easily update measurement codes and related code fragments collectively known as [tags](#) on your website or mobile app. Once the small segment of Tag Manager code has been added to your project, you can safely and easily deploy analytics and measurement tag configurations from a web-based user interface.



When Tag Manager is [installed](#), your website or app will be able to communicate with the Tag Manager servers. You can then use Tag Manager's web-based user interface to set up tags, establish [triggers](#) that cause your tag to fire when certain events occur, and create [variables](#) that can be used to simplify and automate your tag configurations.

A collection of tags, triggers, variables, and related configurations installed on a given website or mobile app is called a [container](#). A Tag Manager container can replace all other manually-coded tags on a site or app, including tags from [Google Ads](#), [Google Analytics](#), [Floodlight](#), and [3rd party tags](#).

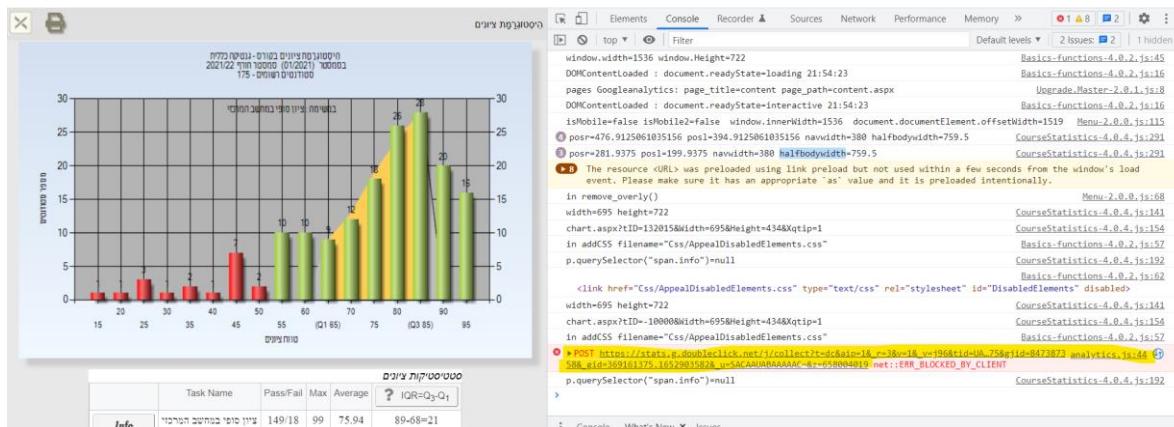
## Consider what tags you will need and where to deploy them

The best practice for every Tag Manager implementation should be to start with an analytics strategy and tag implementation plan. Identify all the tags you have deployed on your existing site or app. For new projects, identify the kinds of tags you will need.

Think about what information you want to collect and determine if there are additional tags you want to deploy. If the data you want to collect is not available, refer to the [developer documentation](#) for information on how to pass additional data to tags.

If all of your tags fire as pages load, and each page has a unique URL, a basic container implementation is sufficient. If your tag firing scenarios are more complex, you may want to implement a more customized container implementation. These custom solutions often implement a [data layer](#), which is code that helps Tag Manager pass data from your site or app to your tags.

בתרמונה: שירות Tag Manager אשר מיושם באתר, מתוך אתר גול, בו מוסבר כי זהו מנגנון הנועד לאסוף מידע בצורה יעילה



בתרמונה: חסימה של קוד השיך ל-'Google Analytics' ע"י חסום פרטומוט שוחתוקן על הדף



The screenshot shows the browser's developer tools open to the 'Elements' tab. The left sidebar lists the DOM structure of the 'index.aspx' page, including sections like 'top', 'grades.txt', 'Accordions', 'Css', 'Header', 'Menu', 'css', 'header', 'hint.css', 'js', 'jsPanel', 'jspanel', 'tableso', and 'index.aspx'. The right pane shows the raw HTML code for the page, which includes various script tags for Google Analytics, CSS files, and JavaScript functions. The code is heavily minified, with some parts like 'Content-Type' and 'Content-Encoding' removed.

```
<!DOCTYPE html>
<html dir="rtl" lang="he">
<head>
    <script src="js/Basics-functions-4.0.2.js"></script>
    <script src="js/fn_info-4.0.3.js"></script>
    <meta name="google-site-verification" content="q9Nk9tPwkJ3eqCQjL9skuNdlwFtdQYjkBKeM" />
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <var upd_external = 99;>
    <link rel="stylesheet" href="hint.css-2.7.0/hint.min.css" media="only screen and (min-width: 600px)" />
    <link rel="stylesheet" href="tablesorter-V2.31.0/theme.ice.min.css" type="text/css" />
    <!-- Global site tag (gtag.js) - Google Analytics -->
    <script async src="https://www.googletagmanager.com/gtag/js?id=UA-112057216-1"></script>
    <link href="https://fonts.googleapis.com/css?family=Oleo+Script" rel="stylesheet" type="text/css" />
    <script src="https://translate.google.com/translate_a/element.js?cb=googleTranslateElementInit&hl=en"></script>
    <script src="js/Upgrade.Master-2.0.1.js" type="text/javascript"></script>
    <script type="text/javascript">
        if (document.all) window.location = "ie7.aspx";
    </script>
    <link rel="stylesheet" href="jspanel-4.13.0/jspanel.min.css" />
    <link rel="stylesheet" href="jsPanel/jsPanel-2.0.2.js" type="text/javascript" />
    <link href="tablesorter-V2.31.0/theme.ice.min.css" rel="stylesheet" type="text/css" />
    <link type="text/css" href="css/Upg...>
```

בתרומה: עניינית קוד מתוך שירות Google Tag Manager בכניסה לאתר

בתמונה: תיוגים שונים שמודדים לפחות חלק מהקוד שרצ באתר

The screenshot shows the Network tab in the Chrome DevTools. A large JSON object is being displayed, representing a response from a Google Analytics endpoint. The object contains various tracking parameters and session information. The JSON is heavily obfuscated with underscores and numbers, making it difficult to read the original code. The DevTools interface includes a sidebar with breakpoints and a bottom bar showing the current line of code.

Sources tab showing the code for `Upgrade.Master-2.0.1.js`. The code includes logic for Google Analytics tracking:

```

1 "use strict";
2 function gtag() { datalayer.push(arguments); }
3
4 if ('upd_external' in window) {
5   var path = location.pathname.toLowerCase();
6   if (path.substr(0, 1) === '/') path = path.substr(1);
7   var title = path.substr(0, path.indexOf('.'));
8   console.log("pages_GoogleAnalytics: page_title=" + title + " page_path=" + path);
9
10 window.dataLayer = window.dataLayer || [];
11 gtag('js', new Date());
12
13 gtag('config', 'UA-112057216-1', {
14   'page_title': title,
15   'page_path': path,
16   'groups': 'default'
17 });
18
19
20 function googleTranslateElementInit() {
21   new google.translate.TranslateElement({
22     pageLanguage: 'iw',
23     includedLanguages: 'en,zh-CN,zh-TW,ru,ar,fr,de,it,pt,es,yi,iw'
24   }, 'google_translate_element');
25 }
26
27 function fn_toheb() {
28   var helocation = window.location.href.toLowerCase().replace("eng.aspx", ".aspx");
29   window.location = helocation;
30 }

```

Sources tab showing the code for `Index-2.0.7.js`. The code includes logic for Google Analytics tracking:

```

97 }
98
99 function google_analytics_publist_last_mounth(e) {
100   var el = e.target;
101   var sem = el.getAttribute('data-sem');
102   var coursenumber = el.innerHTML;
103   var CourseName = el.closest('td').nextSibling.innerText;
104   console.log("CourseName =" + CourseName);
105   var greadview = el.closest('table').getAttribute('id').toLowerCase();
106   var i = greadview.indexOf('gridview');
107   var id = greadview;
108   if (i > 0) id = greadview.substr(i + 9);
109   console.log('sem=' + sem + ' coursenumber=' + coursenumber + ' CourseName=' + CourseName + ' id=' + id);
110   gtag('event', 'Grades', {
111     'event_category': 'publish last mounth-' + id,
112     'event_label': sem,
113     'Semester': sem,
114     'CourseNumber': coursenumber,
115     'CourseName': CourseName
116   });
117 }

```

בתרומה: בניית מידע על הקורסים באמצעות שירותי גוגל

Sources tab showing the code for `Index-2.0.7.js`. The code includes logic for Google Analytics tracking:

```

115   'coursenumber': coursenumber,
116   'CourseName': CourseName
117 };
118 function google_analytics_smart(e) {
119   var id = e.target.id;
120   if (id === '') {
121     let el = e.target;
122     var parent = el.closest('[class*="smart"]');
123     if (parent) {
124       console.log(' nodename =' + parent.nodeName + ' parentID=' + parent.id);
125       id = parent.id;
126     }
127   }
128   console.log(' id=' + id);
129   gtag('event', 'Grades', {
130     'event_category': 'CourseSmarts',
131     'event_label': id
132   });
133 }
134
135 _domReady(function () {
136   _trigEvent(document, "button.info", fn_info, _uEvent);
137   _trigEvent(document, "button.staffmail", fn_staffmail, _uEvent);
138   _trigEvent(document, "#PlayVideo", PlayVideo, _uEvent);
139
140   if ('upd_external' in window) {
141     _trigEvent(document, '.ga-1', google_analytics_publist_last_mounth, _uEvent);
142     _trigEvent(document, '.smart', google_analytics_smart, _uEvent);
143   }

```

Screenshot showing browser developer tools and network traffic analysis.

**Top Panel:** Network tab showing requests to grades.technion.ac.il. One request (line 160) is highlighted in yellow, containing Hebrew text about Moodle usage.

```

132 });
133 }
134
135 _domReady(function () {
136   _trigEvent(document, "button.info", fn_info, _uEvent);
137   _trigEvent(document, "button.staffmail", fn_staffmail, _uEvent);
138   _trigEvent(document, "#PlayVideo", PlayVideo, _uEvent);
139
140   if ('upd_external' in window) {
141     _trigEvent(document, '/gal', google_analytics_publist_last_mounth, _uEvent);
142     _trigEvent(document, '/smart', google_analytics_smart, _uEvent);
143   }
144   var moodle = document.querySelectorAll(".moodlescan");
145   moodle.forEach(m => { tooltipMoodle(m); })
146
147 });
148
149
150 function tooltipMoodle(el) {
151   const moodleContent = '' +
152     '<div style="padding-right:20px;padding-top:0">' +
153       '<br>&nbsp;' +
154       'אתה זוכה על ידי המלצה מנהמכת במכון סרינה' +
155       ' Moodle <br>&nbsp;' +
156       '+ לא יחויבו בתשלום Moodle אשי בהחרות מוסרים מ' +
157       '<br>&nbsp;' +
158       '+ ציירנו בחלון תמחורנות כאשר לא רוצה יותר' +
159       '<br/>&nbsp;&nbsp;&nbsp;&nbsp;+' +
160       '+ בקרים אדו יבואו מחרות ריקות כמו פונתת המזגה הבא'

```

**Middle Panel:** Browser screenshot of grades.technion.ac.il/index.aspx. The page header includes the Technion logo and the text "ביחס הבאים ל- Grade - Grade - מינוחת האיזום בקורס בתופסomi (ע.)".

**Bottom Panel:** Network tab in Chrome DevTools showing session cookies for grades.technion.ac.il. A cookie named '\_ga' is highlighted in yellow.

בתמונה: עוגיות המשיכות לשירותי גול שנשלחות עם בקשה לצפיה במידע על ציונים

Screenshot of Burp Suite showing network traffic analysis.

**Request:** A POST request to /collect?&i=2&id=G-WRR46JN9W2... with parameters \_id=11205721&\_t=1649581096. The response body is in Hebrew and contains session cookies.

**Response:** The response shows the HTML content of the page, including the Hebrew message from the screenshot above.

**Inspector:** Shows Request Attributes, Request Query Parameters, Request Cookies, Request Headers, and Response Headers. The '\_ga' cookie is visible in the Request Cookies section.

Burp Suite interface showing a list of captured requests and their details. The list includes various Google Analytics and Translate API requests from different hosts and ports.

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP
359	https://www.google-analytics.com	POST	/g/collect?v=2&tid=G-WRR46JN9W2...		✓	204	550	text		בקרים - מס' נזירים ב...	✓	142.250.185.142	
353	https://grades.technion.ac.il	GET	/chart.aspx?ID=-10000		✓	200	7975	HTML	aspx		✓	132.68.239.19	
351	https://translate-pa.googleapis.com	GET	/v1/supportedLanguages?client=te&dis...		✓	200	14363	script	js		✓	142.250.185.138	
350	https://www.google-analytics.com	GET	/analytics.js			200	50809	script	js		✓	142.250.185.142	
346	https://translate.googleapis.com	GET	/_/translate_http/_/js/k=translate_htt...			200	230134	script	js		✓	142.250.181.234	
339	https://www.googletagmanager.com	GET	/gtag/s?id=UA-11205726-1		✓	200	104891	script	js		✓	142.250.181.232	
329	https://grades.technion.ac.il	GET	/GET/1.0.0.js			200	2187	script	js		✓	132.68.239.19	
328	https://grades.technion.ac.il	GET	/js/Scan-3.0.js			200	7534	script	js		✓	132.68.239.19	
338	https://grades.technion.ac.il	GET	/js/CourseStatistics-4.0.4.js			200	14149	script	js		✓	132.68.239.19	
326	https://translate.google.com	GET	/translate_a_element.js?cb=googleTra...		✓	200	78516	script	js		✓	142.250.181.238	
321	https://www.google-analytics.com	POST	/g/collect?v=2&tid=G-WRR46JN9W2...		✓	204	550	text			✓	142.250.185.142	
320	https://www.google-analytics.com	GET	/analytics.js			200	50809	script	js		✓	142.250.185.142	
319	https://translate-pa.googleapis.com	GET	/v1/supportedLanguages?client=te&dis...		✓	200	14363	script	js		✓	142.250.185.138	
318	https://www.googletagmanager.com	GET	/gtag/s?id=G-WRR46JN9W2&l=data...		✓	200	194157	script	js		✓	142.250.181.232	

Request Response Inspector

```

%A%07%9A%D7%9E%D7%95%D7%AA%20%D7%9C%D7%9B%D7%A7%
D7%A6%D7%95%D7%A2%20%D7%A9%D7%94%D7%AA%D7%86%D7%97%
%D7%9A%D7%95%20%D7%91%D7%A1%D7%9E%D7%A1%D7%98%D7%A
8%_s=1 HTTP/2
2 Host: www.google-analytics.com
3 Content-Length: 243
4 Sec-Ch-Ua: "(Not a Brand";v="8", "Chromium";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.51 Safari/537.36
7 Sec-Ch-Ua-Platform: "Linux"
8 Content-Type: text/plain; charset=UTF-8
9 Content-Transfer-Encoding: binary
10 Origin: https://grades.technion.ac.il
11 Sec-Fetch-Site: cross-site
12 Sec-Fetch-Mode: no-cors
13 Sec-Fetch-Dest: empty
14 Referer: https://grades.technion.ac.il/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17
18 empage_view
19 emHistogram & et=23|4ep.event_category=Final&
ep.event_label=
%D7%A5%D7%99%D7%95%D7%9F%20%D7%A1%D7%95%D7%A4%D7%9
%20%D7%91%D7%9E%D7%97%D7%A9%D7%91%20%D7%94%D7%9E%
D7%A8%D7%98%D7%96%D7%99
20 emscroll_&et=171&epn.percent_scrolled=90

```

בתמונה: שיתוף אוטומטי של היסטוגרמה עם Google Analytics

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP
350	https://www.google-analytics.com	GET	/analytics.js			200	50809	script	js		✓	142.250.185.142	
321	https://www.google-analytics.com	POST	/g/collect?v=2&tid=G-WRR46JN9W2...	✓		204	550	text			✓	142.250.185.142	
320	https://www.google-analytics.com	GET	/analytics.js			200	50809	script	js		✓	142.250.185.142	
293	https://www.google-analytics.com	POST	/g/collect?v=2&tid=G-WRR46JN9W2...	✓		204	550	text			✓	142.250.185.142	
292	https://www.google-analytics.com	POST	/g/collect?v=2&tid=G-WRR46JN9W2...	✓		204	550	text			✓	142.250.185.142	
283	https://www.google-analytics.com	POST	/j/collect?v=18,_v=j96&a=274544334...	✓		200	623	text			✓	142.250.185.142	
282	https://www.google-analytics.com	POST	/g/collect?v=2&tid=G-WRR46JN9W2...	✓		204	550	text			✓	142.250.185.142	
280	https://www.google-analytics.com	GET	/analytics.js			200	50809	script	js		✓	142.250.185.142	
254	https://www.google-analytics.com	POST	/g/collect?v=2&tid=G-WRR46JN9W2...	✓		204	550	text			✓	142.250.185.142	
251	https://www.google-analytics.com	GET	/analytics.js			200	50809	script	js		✓	142.250.185.142	
218	https://www.google-analytics.com	POST	/g/collect?v=2&tid=G-WRR46JN9W2...	✓		204	550	text			✓	142.250.185.142	
215	https://www.google-analytics.com	POST	/g/collect?v=2&tid=G-WRR46JN9W2...	✓		204	550	text			✓	142.250.185.142	
211	https://www.google-analytics.com	POST	/j/collect?v=18,_v=j96&a=461839328...	✓		200	623	text			✓	142.250.185.142	
210	https://www.google-analytics.com	GET	/analytics.js			200	50809	script	js		✓	142.250.185.142	

בתמונה: כמוות תעבורת גבוהה ל-Google Analytics- בגלישה במשרץ של בדקה באתר היצונים

## Null Session + RPC Default Credentials

ביצענו ניסיון לנצל את העבודה ששרת upgrade-tcp האזין לפניות בפורט 135/TCP/RPC כדי לבצע חיבור אNONYMI-L RPC שלו מבלי לספק שם ומשתמש וסיסמה בעלי הרשאה לכך אף אם שניתן לראות בצלום המסר מנגנון זה נחסמ ע"י האדמין של השרת:

```

File Actions Edit View Help
(kali㉿kali)-[~]
$ rpcclient -U '' -N 132.68.3.58
Cannot connect to server. Error was NT_STATUS_ACCESS_DENIED

```

אצל מחשבים שמותקנת עליהם מערכת הפעלה של Microsoft Windows מוגדרים

```
C:\WINDOWS\system32\cmd.exe

C:\Users\kfir2>net use \\132.68.3.58\IPC$ "" /user:
System error 5 has occurred.

Access is denied.

C:\Users\kfir2>net use \\132.68.3.58\IPC$
The password or user name is invalid for \\132.68.3.58\IPC$.

Enter the user name for '132.68.3.58': admin
Enter the password for 132.68.3.58:
System error 1326 has occurred.

The user name or password is incorrect.
```

כברירת מחדל מספר שיתופים חבויים, אחד מהם ה-\$IPC שמיועד לתקשורת בין תהליכים (Inter-process communication Null Session (כלומר מבלי לספק משתמש מורשה וסיסמה) אך גם זה לא צלח:

הצלחנו לקבל מהשרת מידע על כל השיתופים החבויים שמוגדרים עליו, بما שניכן לראות בתמונה הבאה:

גם ניסיון לגשת אליו מבלי לספק פרטי ההזדהות עליה בתהו, אך בזכות מידע זה אנחנו יודעים שככל הנראה סריקות המבחנים נשמרות בשיטוף \$scanner.

ניסיון ליצור Remote shell של powershell בעזרת הכלי האדמיניסטרטיבי של מיקרוסופט psexec שמשתמש ב-\$IPC גם כן דרש משתמש בעל הרשות ולכן לא צלח.

#### -התחברות ל-FTP של שרת הציגנים

לאחר שראינו שפורט ה-FTP של שרת ה-\$IPC (upgrade-PRD.cc.technion.ac.il) פותח ונכניתן לגשת אליו מתוך הרשות הטכניתית המאובטחת, ניסינו והצלחנו להתחבר ב-FTP anonymous אל השרת בערך משתמש מוגדר בשם ftp (לא נדרש סיסמה).  
למשתמש זה אמם לא הייתה הרשות לשינוי/מחיקה/יצירת קבצים ותיקיות על גבי השרת, אך הייתה לו גישה למספר תיקיות שנכנית היה לעבור ביניהן ולהציג את תוכנן כפי שנכנית לראות בצלומי המסך למטה. המעניינת מביניהם הייתה תיקיית GR שבה אנו מכנים שנמצא מסד הנתונים של השרת, אך לא הייתה המשתמש שלנו גישה להציג את תוכנה.

```
C:\WINDOWS\system32\cmd.exe - ftp 132.68.3.58
ftp>
ftp> cd system_web
250 CWD command successful.
ftp> pwd
257 "/aspnet_client/system_web" is current directory.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
05-01-20 04:30PM <DIR> 4_0_30319
226 Transfer complete.
ftp: 53 bytes received in 0.01Seconds 5.30Kbytes/sec.
ftp> put 1.txt
200 PORT command successful.
550 Access is denied.
ftp> mkdir my_folder
550 Access is denied.
ftp>
ftp> cd 4_0_30319
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp> mkdir my_folder
550 Access is denied.
ftp> put 1.txt
200 PORT command successful.
550 Access is denied.

```

---

```
C:\WINDOWS\system32\cmd.exe - ftp 132.68.3.58
C:\Users\fir2\ftp 132.68.3.58
Connected to 132.68.3.58.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (132.68.3.58:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
ftp>
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
05-01-20 04:30PM <DIR> aspnet_client
03-31-22 08:00AM <DIR> GR
226 Transfer complete.
ftp: 100 bytes received in 0.00Seconds 100000.00Kbytes/sec.
ftp> pwd
257 "/" is current directory.
ftp> put 1.txt
200 PORT command successful.
550 Access is denied.
ftp> mkdir my_folder
550 Access is denied.
ftp>
ftp> cd GR
550 Access is denied.
ftp>
ftp> cd aspnet_client
250 CWD command successful.
ftp>
ftp> pwd
257 "/aspnet_client" is current directory.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
05-01-20 04:30PM <DIR> system_web
226 Transfer complete.
ftp: 54 bytes received in 0.00Seconds 54000.00Kbytes/sec.
ftp> mkdir my_folder
550 Access is denied.
ftp> put 1.txt
200 PORT command successful.
550 Access is denied.
```

### התחברות ל-FTP של שרת comsign

שרת זה משמש לחתימה דיגיטלית של מסמכים כגון תעודה ציונית, ומכוון הרלוונטיות שלו בלבד, השימושו לארגון והאינטראס להגן עליו ברורה.

בצילומי המסקן ניתן לראות שקיימים אצלו מספר לא קטן של פורטים פתוחים ופרטם: **Anonymous FTP**, ושגם אליו ניתן לבצע:

```
└$ nmap -sV comsign.cc.technion.ac.il
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-18 13:25 EDT
Nmap scan report for comsign.cc.technion.ac.il (132.68.3.76)
Host is up (0.071s latency).
rDNS record for 132.68.3.76: ComSign.cc.technion.ac.il
Not shown: 987 filtered tcp ports (no-response), 5 filtered tcp ports (host-unreach
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftptd
135/tcp   open  msrpc        Microsoft Windows RPC
443/tcp   open  ssl/http    Microsoft IIS httpd 10.0
445/tcp   open  microsoft-ds?
1801/tcp  open  msmq?
2105/tcp  open  msrpc        Microsoft Windows RPC
2107/tcp  open  msrpc        Microsoft Windows RPC
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
└─$ ftp comsign.cc.technion.ac.il
Connected to ComSign.cc.technion.ac.il.
220 Microsoft FTP Service
Name (comsign.cc.technion.ac.il:kali): ftp
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> █
```

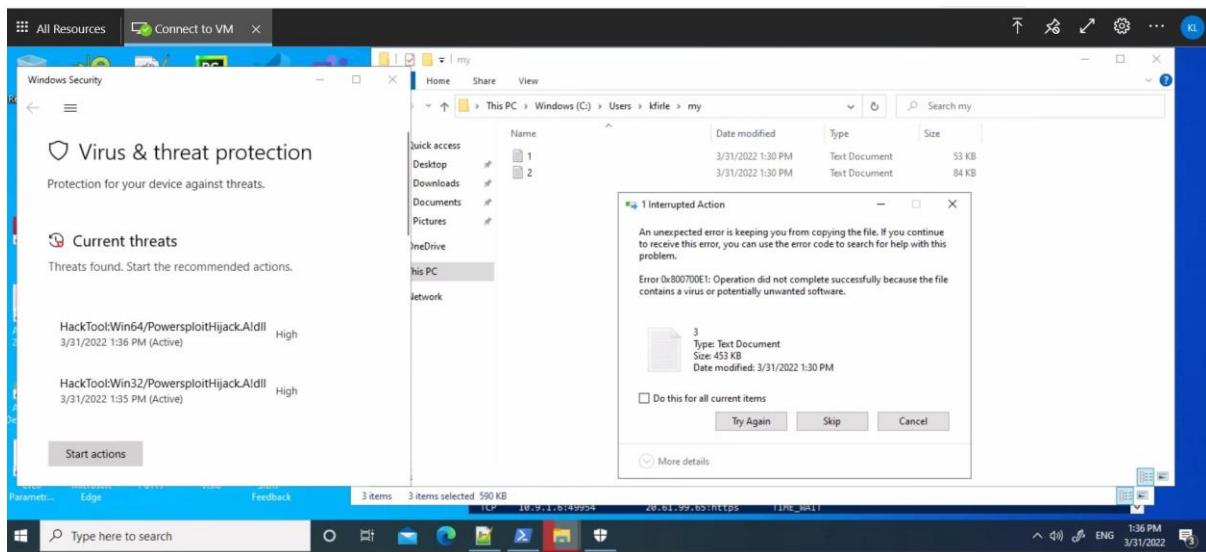
בתמונה: שירות ftp פתוח מול שרת החתימות הדיגיטליות של הטכניון, המאפשר חיבור אונימי (ללא הרשות)

## - ניסיון Privilege Escalation ב-VDI

בזיהו נוסף שהחלנו לבדוק היה ניסיון לגashת למערכת הצלינים דרך מחשב וירטואלי (Virtual Desktop) שנג-ish עבר סטודנטים שחילק משירותי ה-IT שהטכניון מציע. להפתעתנו גילינו בדף האתר: <https://whatismyipaddress.com/> שבכתובת ה-IP שבה המחשב הווירטואלי משתמש ב-WAN (לאחר ביצוע NAT) אינה נמצאת פיזית בטכניון אלא במרכז שירותי של מיקרוסופט שנמצא בהולנד. למרות שהוא חלק מ-subdomains של הטכניון (staff) מהמחשב הווירטואלי לא הייתה גישה לכל מערכות הצלינים, ובפרט אפילו לא לאתר grades שלו בסטודנט יכול להתחבר ללא צורך בחיבור לרשת הטכניונית. על המשתמשים שלנו הוחלו הקשחות policy group שהסנו גישה ל-cmd, ל-registry ול-control panel אך הצליחו להתחבר על בר חלקית ע"י שימוש ב-powershell שאינם חסום שם. הצליחו לגלוות של-admin המקומי שמודדר על המחשבים הווירטואליים נקרא techadmin, ומצביעו שהם הותקנו במרובץ (ככל הנראה מאותו אימג'), קיוינו למצוא את הסיסמה שלו בקובץ \Windows\Panther\unattend.xml: C:\Windows\Panther\unattend.xml. מתוך כוונה לבדוק האם זהו האדמין המקומי גם בשרתים של מערכות הצלינים. צערכנו בשדה הרלוונטי לסיסמת האדמין בקובץ הופיע הטקסט הבא:

```
<AdministratorPassword xmlns:msxsl="urn:schemas-microsoft-com:xslt"
xmlns:rdf="http://schemas.microsoft.com/2009/05/WindowsAzure/ServiceManagement"
xmlns:wa="http://schemas.microsoft.com/windowsazure">*SENSITIVE*DATA*
DELETED*</AdministratorPassword>
```

השלב הבא היה שניסינו לשימוש במספר כל' פריצה מוכרים שמרתם privilege escalation במילוי השגת הרשות אדמין, בין היתר נבדקו: mimikatz, privsec, krbrelay :windows defender crackMapExec-I



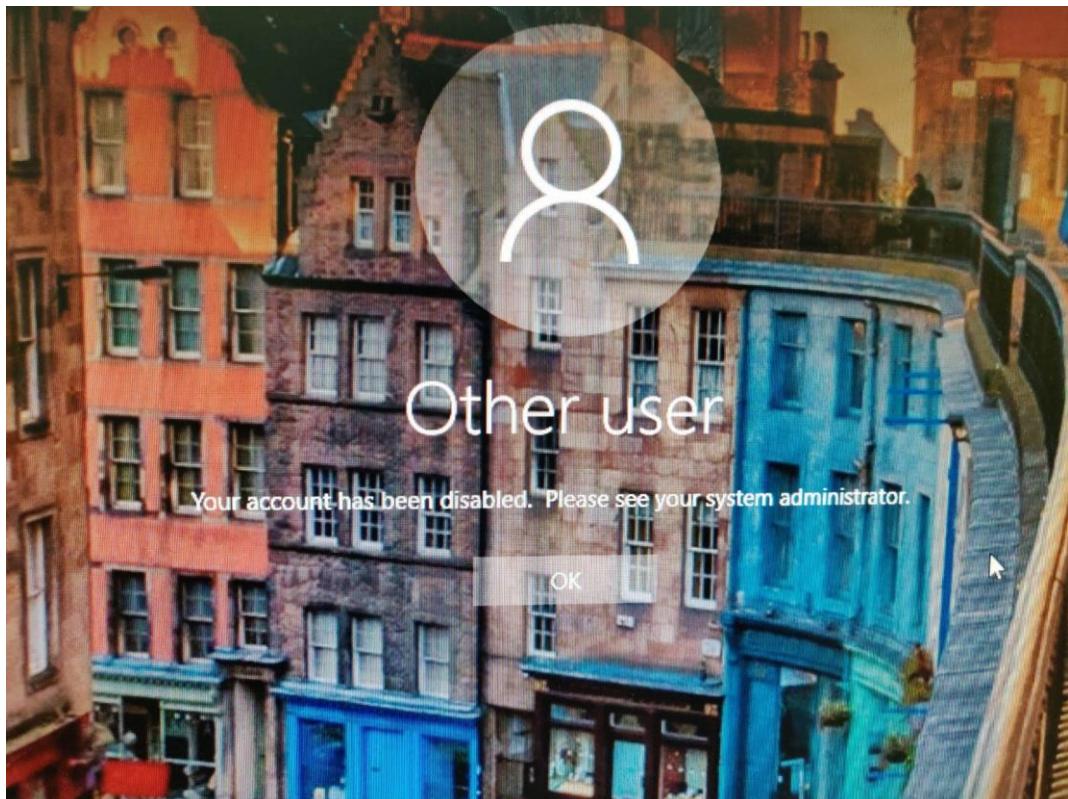
### נסיין להתחבר ל-LAN של שרת הצלינים ולהאזין לתעבורה

לאחר שהגילינו כי קיים שירות ftp על-גבי שרת הצלינים UPGRADE,ניסינו להגיע למצב בו אנו מתחברים לרשת המקומיית ומצליחים להאזין לתעבורה העוברת ברשת (ואף לנסיין התחברות לשירות ה-ftp על-מנת לקבל את ה-Credentials המשמשים לחיבור), שכן זהו שירות לא מוצפן.

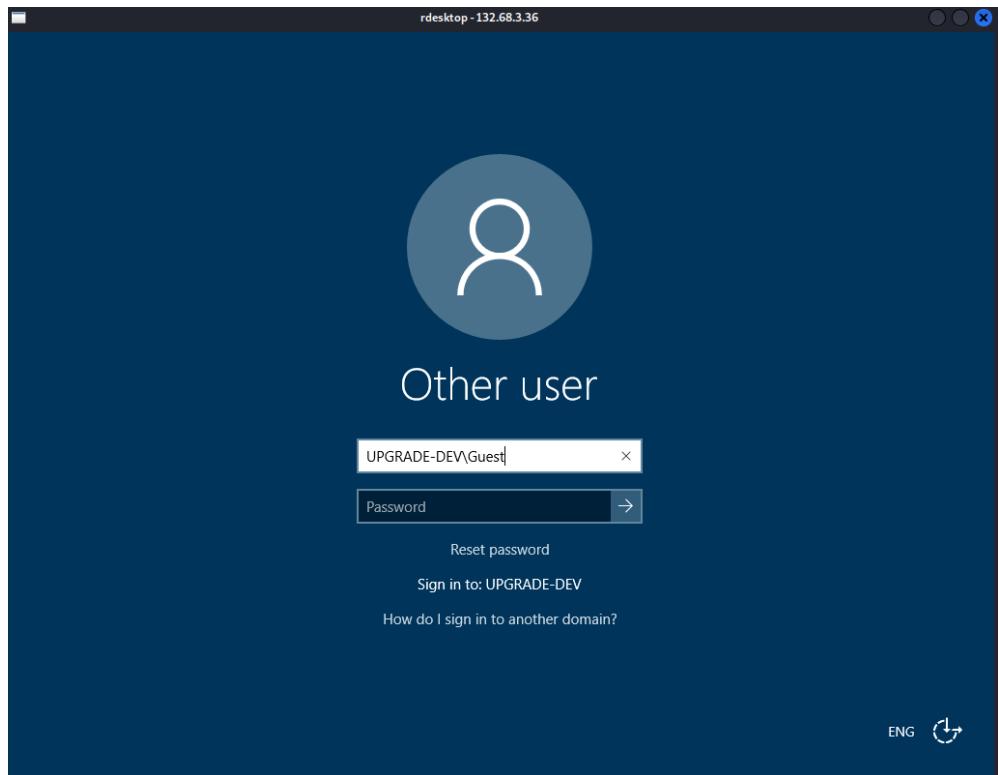
ניסינו להתחבר ממספר מעבדות ומקומות בטכניון, כולל ניסיונות למצוא פיזית את המיקום של השרת, ללא הצלחה. מסתמן כי הרשות בה נמצא השירות מופרדת משאר הרשותות הגלויות, ביןיהן TechSec על-שלל תתי הרשותות שבה.

### נסיין לבצע ARP Poisoning ברשת פנימית בפקולטה כדי לקבל הרשותות גבוהות ולהתקדם ברשת

מתוך רצון להגיע לדומיין המכיל את שרת הצלינים, ניסינו לקבל גישה עם הרשותות גבוהות בדומיין אחר אליו יש לנו גישה פיזית, כדוגמת מעבדה בפקולטה למדעי המחשב. ראשית, נציג לנו בדומייניהם שבדקנו, אין אפשרות להתחברות כאורוח:

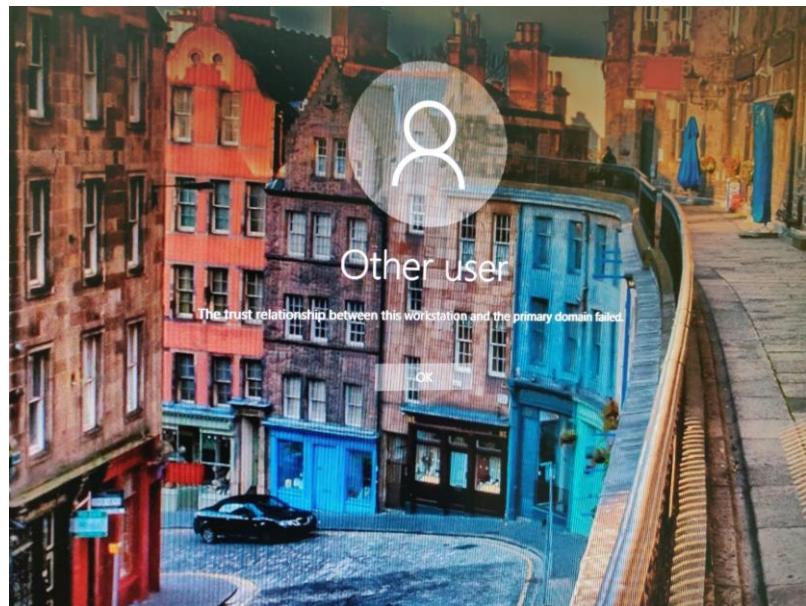


בתמונה: נסיוןהתחברות עם משתמש Guest במעבדה לפתיחת תוכנה



בתמונה: נסיוןהתחברות עם משתמש Guest בשירות remote desktop על גבי שרת הצלינים UPGRADE - מוביל לאוthonה הודעה

במו כן, אין חיבור ממשי בין הדומיינים:



בתמונה: נסיון התחברות עם משתמש טכניוני על מחשב במעבדה לפיתוח תוכנה

דרך אחת שניסינו היא ביצוע ARP Poisoning ברשת פנימית (זופף הודעת ARP בה אנו "מודיעים" על פני הרשת כי המחשב שלנו הוא בעל כתובת הפיזית המתאימה לבכנתה ה-IP של הנטב וגם של הקורבן, כך שנוכל לשמש MiTM).

Sequence	Source MAC	Destination MAC	Type	Content
284 14.746609	VMware_e4:d6:1a	ASUSTekC_47:75:c0	ARP	60 132.68.39.254 is at 00:0c:29:e4:d6:1a
285 14.746624	VMware_e4:d6:1a	ASUSTekC_47:75:c0	ARP	60 132.68.39.254 is at 00:0c:29:e4:d6:1a
286 14.746743	VMware_e4:d6:1a	HewlettP_70:66:d6	ARP	60 132.68.36.70 is at 00:0c:29:e4:d6:1a
287 14.746753	VMware_e4:d6:1a	HewlettP_70:66:d6	ARP	60 132.68.36.70 is at 00:0c:29:e4:d6:1a

בתמונה: שילוח הודעות ARP על פני הרשת המתחזקת לנטב ולקורבן

כאשר ביצענו את שילוח הودעת ARP, גלינו כי הנטב שלוח מידית הודעת אזהרה, מלאה בהודעת "תיקון" המבטלת את המתקפה:

▼ Address Resolution Protocol (ARP Announcement)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
[Is gratuitous: True]
[Is announcement: True]
Sender MAC address: HewlettP_70:66:d6 (44:31:92:70:66:d6)
Sender IP address: 132.68.39.254
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 132.68.39.254
▼ [Duplicate IP address detected for 132.68.39.254 (44:31:92:70:66:d6) - also in use by 44:31:92:30:7f:ae (frame 495)]
▼ [Frame showing earlier use of IP address: 495]
▼ [Expert Info (Warning/Sequence): Duplicate IP address configured (132.68.39.254)]
[Duplicate IP address configured (132.68.39.254)]
[Severity level: Warning]
[Group: Sequence]
[Seconds since earlier frame seen: 2]
3879 73.743988     HewlettP_35:fd:e8     Broadcast     ARP     60 ARP Announcement for 132.68.39.254 (duplicate use of 132.68.39.254 detected!)
3880 73.744903     HewlettP_30:7f:ae     Broadcast     ARP     60 Gratuitous ARP for 132.68.39.254 (Reply) (duplicate use of 132.68.39.254 detected!)
3881 73.745201     HewlettP_70:66:d6     Broadcast     ARP     60 Gratuitous ARP for 132.68.39.254 (Reply)

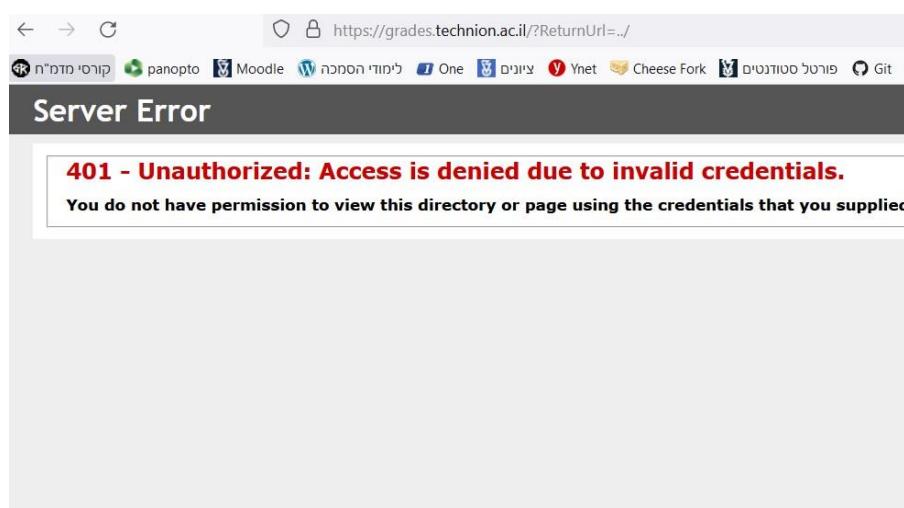
עם זאת, נצין שקיימות דרכים יותר בטוחות למניעת מתקפה שכזו, בין היתר, ניתן להגדר בכל פורט פיזי במעבדה ב-VLAN שבן המטריה המרכזית של נקודות החיבור במעבדה היא לאפשר חיבור יציב לאינטרנט עבור משתמשים ולא לטובות תקשורת בין מחשבים במעבדה.

Host List <span style="float: right;">X</span>		
IP Address	MAC Address	Description
132.68.36.204	44:31:92:55:F4:E8	
132.68.36.153	A8:9C:ED:40:4D:C5	Android-5.local
132.68.36.70	30:5A:3A:47:75:C0	Boaz-cggc-pc.local
fe80::f68e:38ff:feb1:9bed	F4:8E:38:B1:9B:ED	crypto34.local
fe80::4a4d:7eff:fe9b:862d	48:4D:7E:9B:86:2D	crypto35f.local
fe80::4a4d:7eff:fe9d:ef90	48:4D:7E:9D:EF:90	crypto36f.local
fe80::f68e:38ff:feaf:5ff	F4:8E:38:AF:05:FF	crypto37f.local
fe80::e68e:38ff:fe84:6bbb	E4:8E:38:84:6B:BB	crypto38f.local
132.68.36.20	00:25:90:34:4E:13	gip-main.local
132.68.39.119	00:08:9B:D2:5A:4C	ISL-NAS.local
fe80::b226:28ff:feda:d210	B0:26:28:DA:D2:10	knuth.local
132.68.36.36	D8:CB:8A:06:47:51	LCCN-12.local
fe80::ac7a:d8fe:a056:bf64	D8:CB:8A:06:47:51	LCCN-12.local
132.68.39.95	24:5E:BE:51:09:AB	rambo-qnap.local
132.68.39.18	24:5E:BE:37:AC:3E	walkure.local
<a href="#">Delete Host</a>		<a href="#">Add to Target 1</a>
DHCP: [B8:CA:3A:85:27:2C] REQUEST 132.68.36.131 Randomizing 1023 hosts for scanning... Scanning the whole netmask for 1023 hosts... 237 hosts added to the hosts list... DHCP: [B8:CA:3A:85:27:2C] REQUEST 132.68.36.131 DHCP: [E6:DD:B9:F5:3E:EE] REQUEST 132.68.36.18		

בתמונה: סריקה של המחשבים ברשת המקומית של המעבדה לפתיחת תוכנה והאזנה לביקשות DHCP ממשתמשים חדשים המctrivers לרשף

### נסיין Directory Traversal וגישה לקבצים

כאמור, כל בקשה גישה לדף כלשהו ב-Grades מלאה בעוגיות זהירות והאימות, אך שלא מתאפשר Directory Traversal.



עם זאת, בחלק מסוינו לנו למצא דומיינים מיוחדים, מצאנו דומיין אשר כן מתאפשר בו Directory Traversal אך לא נמצא בו דברים "מעניינים":

The screenshot shows a dark-themed web browser window. At the top, the address bar displays the URL: `webdev.web3.technion.ac.il/docs/cis/`. Below the address bar is a navigation bar with icons for back, forward, and search, followed by a lock icon indicating a secure connection. Underneath the navigation bar is a horizontal menu bar with several items: `Technion`, `Downloads`, `Music`, `Learning`, `Bicycle`, `Food`, `Shop`, and `Watch`. The main content area of the browser shows the title **Index of /docs/cis**. Below the title is a table listing files and directories:

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">private/</a>	2015-02-11 09:49	-	
<a href="#">public - Shortcut.lnk</a>	2018-05-10 10:35	1.8K	
<a href="#">public/</a>	2020-11-18 11:23	-	

## מסקנות והמלצות

### הורדת האתר Tadpis מהרשת

אנו ממליצים להוריד לוחטין את המערכת המיוישנת לצפייה בגלוין הציוניים מהאינטרנט. מכיוון שאופן ההזדהות נעשה ב프וטוקול לא מאובטח (HTTP) - מה שמאפשר האذנה וקבלת ה-Credentials ע"י כל אחד שמחובר לאותה הרשות (לדוגמא דרכו רשות TechSec) ומכוון שמרחב הסיסמאות קטן מאוד וצפוי, מה שהופך את יכולת לגלוות את הסיסמה ולקבל את גלוין הציוניים המפורט של כל סטודנט בטכניון למשימה קלה עברו תוקף.

### סגירת פורטים לא הברחיים

ראינו במאן קל למצוא את כל ה-Sub-Domains הרשמיים תחת הטכניון (בצירוף כתובות ה-IP שלהם). ניתן בקלות לבתוב סקריפט שסורק את כל הכתובות הללו ובודק אילו פורטים פתוחים. אנו ממליצים לבצע בדיקה נוספת של כל השירותים ולודא כי אין פורטים מיוחדים שפתוחים.

### ביטול יבולת חיבור אונימי ל-ftp ומעבר לשירות ftp מאובטח

אם נס למשתמש האונימי אין הרשות קריאה וכתיבה בשרת ה-ftp, אך זהה אינה פרקטיקת טובות לאפשר חיבור ללא אימוט לכל משתמש שהוא לשירות של משאב קריטי.

יתכן גם כי בעמידה תגלה חולשה המאפשרת Privilege Escalation מחיבור אונימי, אך שרכי צמצם את משטח התקיפה על-ידי ביטול האפשרות. כמו כן, אין סיבה להמשיך להשתמש ב프וטוקול ישן ולא מאובטח, באשר יש חולופה הולמת ומאובטחת יותר כמו **sftp**

### הגבלת גישה ל-UPGRADE לפי Username

במצב הנוכחי כל משתמש שמחובר לרשות הטכניונית המאויבטחת יכול לגשת לדף ההתחברות של אתר upgrades למטרות שהוא מיועד לסגל בלבד. מכיוון שבעת ההתחברות לרשות המאויבטחת המשתמש מדין את פרטי היזהו שלו, במהלך הגלישה ברשות ניתן להזמין אותה ולהציג לו גישה רק למשאים שאיליהם הוא

מורשה. דרך יישום אפשרית היא ע"י Firewall שמבצע סינון תעבורת גם לפי המשתמש ולא רק לפי כתובת ה-IP (למשל Identity Awareness של Cisco), כך שניין להגדיר קבוצה ב-Active directory של מורשי גישה ולהשתמש בה. על אף שלא מדובר בתיקון לפירצת אבטחה, לדעטנו זהו שיפור חיוני שיהווה נדרש נוספת בהגנה על המערכת.

#### **יישום VLAN במעבדות הטכניוניות**

כפי שפירטנו, בכל מקום בו קיימת אפשרות להתחבר לפורט פיזי עם מחשב נייד, ניתן לישם מנגנון של VLAN על גבי ה-Switches בשכבה 2, כך שכל פорт פיזי המאפשר התחברות לרשת פנימית בלבד, ישמש ברשות מבודדת ולא יוכל האזנה לתעבורה ויכולת זיווף הודעות שעולות להוביל לקבלת גישה לא מורשית למערכת.

עבור מחשבים נייחים במעבדות, מומלץ לישם port-security אשר מבטיח כי רק לבתות MAC מוגדרת מראש תהיה גישה לרשות דרך פорт זה.

#### **הפסקת שליחת נתונים לגוגל**

המליצה באן היא מאוד ברורה - לסטודנט הנרשים לטכניון אין יכולת לבחור לא לשולח את נתונו לשרתி גוגל ברגע שהשירות היחיד לצפיה בזכונים עושה זאת. על-כן, נדרש לבטל את שליחת הנתונים לגוגל ואת השירותים המוטמעים באתר הקיימים. בנוסף מומלץ לבחון מול מפתחי האתר מה מטרת איסוף המידע ואם מתברר שאיסוף המידע הכרחי, לשאול להקים שירות מקומי אשר אוסף את הנתונים ומעבד אותם ונשאר בגבולות הטכניון לשימוש פנימי, תוך שמירה על פרטיות המידע של הסטודנטים.

#### **ביטול יבולת enumeration על-ידי החזרת שגיאה פחות ספציפית**

יכולת מנית משתמשים הרשומים או שייכים לארגון כלשהו מהוות חולשה, שכן בשילוב עם מנגנון בדיקת הזדהות שלא חסום לניסיונות Brute-Force (אשר נציג בהמלצה הבאה) לתוקף נשאר רק לנסوت סיסמות חלשות עבור רשות משתמשים קיימת, מה שמגדיל את הסיכון להצלחה להגעה לפרטי הזדהות של משתמש.

על-כן אנו ממליצים לא לחת מידע נוסף ומיותר בעט נסיון התחברות בושל.

#### **אכיפת חוקים אחידים בכל נסיון הזדהות מול שרת האימונות הטכניוני**

בשיטוטינו במרחבי הכתובות הטכניוניות נחשפנו לאתר שדורש הזדהות טכניונית אך לא מפעיל כל מנגנון למניעת Brute Force.

האתר הנ"ו: <https://upgrade-help.net.technion.ac.il/%d7%a6%d7%99%d7%95%d7%a0%d7%99%d7%9d/>

אנו ממליצים להחיל מדיניות ברורה לאיזה שירות מותר לפנות לשרת ההצדחות הטכניוני ולאכוף עליו חוקים כגון יישום מנגנון מניעת Brute Force, זיהוי בוטים וכו' ...

- צמצום הרשאות של סטודנטים על שרתי הפיקולטה למינימום הדרוש.

לסטודנטים בפיקולטה למדעי המחשב קיימת גישה למספר שירותי ברשות המאובטחת (למשל: `comp.cscomp`). בעזרת המשתמשים שלנו, הצלחנו לגשת לקובץ שבו מוגדרים המשתמשים המקומיים של השירות (`etc/passwd`) ולקראות תוכנו. הקובץ עלול לאפשר ביצוע enumeration `user`, ובכל מקרה מדובר במידע אדמיניסטרטיבי שעדיף שלא יהיה נגיש לסטודנטים וכן לדעתנו כדאי לשנות את הרשאות של הסטודנטים ע"י הורדת הרשאות קראה של תיקיות שנמצאים בהיררכיית עץ הקבצים מעל הפורפיל של הסטודנט. נציין בזאת שאות תוכן הקובץ שבו נשמר ה-`hash` של הסיסמות (`etc/shadow`) לא הצלחנו לקרוא, ושלסטודנטים אין אין הרשאות `root` על השירות במצופה.

## רשימת מקורות:

1. ויקיפדיה, האנציקלופדיה החופשית -

<https://he.wikipedia.org/wiki/XSS>

[https://en.wikipedia.org/wiki/File\\_Transfer\\_Protocol](https://en.wikipedia.org/wiki/File_Transfer_Protocol)

[https://he.wikipedia.org/wiki/Remote\\_Procedure\\_Call](https://he.wikipedia.org/wiki/Remote_Procedure_Call)

[https://en.wikipedia.org/wiki/Remote\\_Desktop\\_Protocol#Features](https://en.wikipedia.org/wiki/Remote_Desktop_Protocol#Features)

[https://he.wikipedia.org/wiki/SMB\\_\(%D7%A4%D7%A8%D7%95%D7%98%D7%95%D7%A7%D7%95%D7%9C\)](https://he.wikipedia.org/wiki/SMB_(%D7%A4%D7%A8%D7%95%D7%98%D7%95%D7%A7%D7%95%D7%9C))

Cloudflare - .2

<https://www.cloudflare.com/learning/access-management/rdp-security-risks/>

Sucuri - .3

<https://sucuri.net/guides/what-is-cross-site-scripting/>

Imperva - .4

<https://www.imperva.com/learn/application-security/sql-injection-sqli/>

<https://www.imperva.com/learn/application-security/arp-spoofing/>

Acunetix - .5

<https://www.acunetix.com/websitesecurity/sql-injection/>

Visuality Systems - .6

<https://visualitynq.com/resources/articles/what-is-smb-what-it-decision-makers-need-to-know/>

Geeks for Geeks - .7

<https://www.geeksforgeeks.org/remote-procedure-call-rpc-in-operating-system/>

SANS ISC InfoSec Forums - .8

<https://isc.sans.edu/forums/diary/ls+it+time+to+get+rid+of+NetBIOS/12454/>

Bright - .9

<https://brightsec.com/blog/lfi-attack-real-life-attacks-and-attack-examples/>

TechTarget - .10

<https://www.techtarget.com/searchnetworking/definition/NetBIOS>

Microsoft - .11

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc940063\(v=technet.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc940063(v=technet.10)?redirectedfrom=MSDN)

.12. ספר הקורס "הגנה ברשות" - אל' ביהם.