פריצת הסיסמה – CTF

פיצחתם את המייל, אנחנו עוד שלב אחד קדימה, בדיוק בשלב האחרון.

הפעם נצטרך לחשוב קצת.

קיבלנו מודיעין של סיסמה מוצפנת **בהצפנת קיסר בהיסט 18**, מה זה אומר,
אנחנו לא מצליחים לפענח אותה...
אולי אתם תצליחו?

אנו יודעים רק שצופן קיסר לוקח כל אות מהטקסט 18 פעמים קדימה בא"ב באנגלית, גם אם נעבור את האות z נחזור לאות a ונמשיך משם לפענח.

שימו לב שאפשר לפרוץ את הצופן רק דרך הסקריפט שנבנה ולא דרך האתר.

הכנו לכם את הקרקע, קראו את העמוד הבא!

שלב 3

הכנו לכם תמונה של תווי ASCII בתיקייה שאתם עובדים עליה.

בתמונה הזאת יש תרגום של כל אות במקלדת למספר דצימלי(המחשב לא באמת מבין אותיות, הוא מבין מספרים, לכן הוא אוטומטית מתרגם את האותיות האלו למספרים שהוא מבין).

למשל האות 'z' שקולה לערך הדצימלי 122, תוכלו לראות זאת בטבלה.

למזלנו על פי המודיעין שקיבלנו, אנחנו נתעסק רק באותיות קטנות, כלומר אותיות בטווח הדצימלי של 97-122 כלומר a עד z.

Code	Char	Code	Char	Code	Char	Code	Char	Code	Char	Code	Char
32	[space]	48	0	64	@	80	P	96	`	112	p
33	!	49	1	65	A	81	Q	97	a	113	q
34	"	50	2	66	B	82	R	98	b	114	r
35	#	51	3	67	C	83	S	99	c	115	s
36	$	52	4	68	D	84	T	100	d	116	t
37	%	53	5	69	E	85	U	101	e	117	u
38	&	54	6	70	F	86	V	102	f	118	v
39	'	55	7	71	G	87	W	103	g	119	w
40	(	56	8	72	H	88	X	104	h	120	x
41	)	57	9	73	I	89	Y	105	i	121	y
42	*	58	:	74	J	90	Z	106	j	122	z
43	+	59	;	75	K	91	[	107	k	123	{
44	,	60	<	76	L	92	\	108	l	124	|
45	-	61	=	77	M	93	]	109	m	125	}
46	.	62	>	78	N	94	^	110	n	126	~
47	/	63	?	79	O	95	_	111	o	127	[backspace]

שלב 3 - המשך

עכשיו נכתוב בפונקציה ()openwebpass, שימו לב לא לגעת איפה שרשום שאסור, זה יכול לפגוע בכל התהליך.

זוכרים איך תקשרנו עם תיבת הטקסט של המייל? עשו זאת שוב רק הפעם השתמשו בתיבת הטקסט **של הסיסמה** ותשימו את התשובה ב-input_pass_box.

עשינו לכם את העבודה של קריאת הסיסמה **המוצפנת שאותה תפענחו.** היא נמצאת במשתנה secret_password.

בנוסף הכנו לכם את answer, כל אות שתצליחו לפענח, פשוט תוסיפו לanswer, כך מוסיפים אות לדוגמה:

```
answer += 'c'
```

כמה כלים אחרונים:

הסיסמה המוצפנת מוצפנת בהיסט 18 בצופן קיסר עם אך ורק אותיות קטנות, רק

דרך האלגוריתם שתבנו אתם תפצחו את הסיסמה. זכרו להשתמש בפונקציה

שהופכת אותיות למספר דצימלי, וכמובן את הפונקציה שהופכת מספר דצימלי לאות

כדי ליצור אפקט מגניב, כל חזרה של לולאה קראו לפונקציה הבאה:

```
send_answer(answer, input_pass_box)
```

הפונקציה שולחת את התשובה שלכם לאתר אבל עוד לא לוחצת Next.

כאשר סיימתם הכול כתבו בשורה האחרונה של הפונקציה ()openwebpass את השורה:

```
send_answer(answer, input_pass_box, True)
```

המשך בעמוד הבא ->

הפונקציה שולחת את התשובה שלכם לאתר אבל הפעם כן לוחצת Next ובודקת את התשובה שלכם מול גוגל!

אם התשובה לא נכונה אתם תראו ב-Pycharm את המשפט "Incorrect Password".

אבל אם התשובה כן נכונה, אתם תדעו שתפסתם את הדגל וניצחתם את האתגר!

אנחנו ממש מחכים שתנצחו כבר, הפריצה הזאת קריטית להצלת נפשות של **עשרות אלפיי אנשים!**