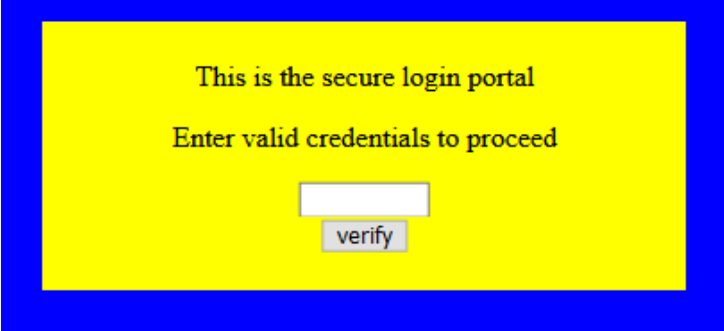


## Mark Seliternikov

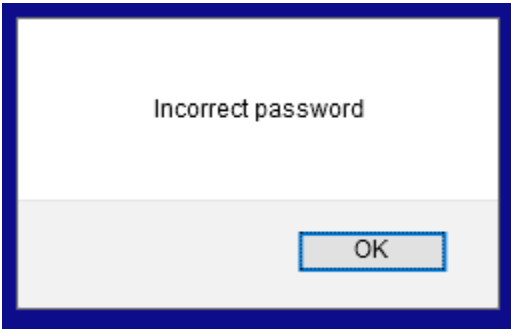
### picoCTF - dont use client side [100 points]

---

# לאתגר זה מקבלים דף שמבקש סיסמה:



# הדף אכן בודק תאימות של הסיסמה לפי מה שנראה:



# חיפשתי קצת בצד לקוח כדי לראות מה קיבלתי (השם של האתגר די אומר מה צריך לעשות).  
# זה מה שמצאתי:

```
function verify() {  
  checkpass = document.getElementById("pass").value;  
  split = 4;  
  if (checkpass.substr(0, split) == 'pico') {  
    if (checkpass.substr(split*6, split*7) == 'a3c8') {  
      if (checkpass.substr(split, split*2) == 'CTF{') {  
        if (checkpass.substr(split*4, split*5) == 'ts_p') {  
          if (checkpass.substr(split*3, split*4) == 'lien') {  
            if (checkpass.substr(split*5, split*6) == 'lz_1') {  
              if (checkpass.substr(split*2, split*3) == 'no_c') {  
                if (checkpass.substr(split*7, split*8) == '9') {  
                  alert("Password Verified")  
                }  
              }  
            }  
          }  
        }  
      }  
    }  
  }  
}
```

# לפי מה שמצאתי ניתן להבין שהחביאו את הסיסמה בצד לקוח ופיצלו לחלקים כדי לגרום לזה להיראות פחות ברור.

# הסיסמה היא הדגל בעצם כי מתחיל ב-pico ואז CTF...

# חיברתי את החלקים וקיבלתי את הסיסמה:

picoCTF{no\_clients\_plz\_1a3c89}

### **מה למדתי**

למדתי משהו פשוט אבל ממש חשוב לגבי אבטחה. אסור לסמוך על הצד לקוח, בשמירת פרטים חשובים (כגון סיסמה) אסור לעשות זאת בצד לקוח. האתגר לא היה קשה אבל הוא מלמד שיעור חשוב שכדאי ללמוד כמה שיותר מוקדם.