

# Laborator III: *Shellcodes* II. Atacuri cu Șiruri de Caractere de Formatare

Iosif George-Andrei

# Tabelă de Conținut

# Tabelă de Conținut

1. Atacuri cu Șiruri de Caractere de Formatare

# Tabelă de Conținut

1. Atacuri cu Șiruri de Caractere de Formatare
2. Exemplu Concret

# Atacuri cu Șiruri de Caractere de Formatare

# Funcționalitate de Formatare

# Funcționalitate de Formatare

- Prezența unor funcționalități de formatare în majoritatea limbajelor de operare (inclusiv în domeniul *web*)

# Funcționalitate de Formatare

- ❖ Prezența unor funcționalități de formatare în majoritatea limbajelor de operare (inclusiv în domeniul *web*)
- ❖ Pentru C, suport oferit prin:



# Funcționalitate de Formatare

- ❖ Prezența unor funcționalități de formatare în majoritatea limbajelor de operare (inclusiv în domeniul *web*)
- ❖ Pentru C, suport oferit prin:
  - ❖ Funcții specifice

# Funcționalitate de Formatare

- ❖ Prezența unor funcționalități de formatare în majoritatea limbajelor de operare (inclusiv în domeniul *web*)
- ❖ Pentru C, suport oferit prin:
  - ❖ Funcții specifice
  - ❖ Șiruri de caractere de formatare

# Funcționalitate de Formatare

- ❖ Prezența unor funcționalități de formatare în majoritatea limbajelor de operare (inclusiv în domeniul *web*)
- ❖ Pentru C, suport oferit prin:
  - ❖ Funcții specifice
  - ❖ Șiruri de caractere de formatare
  - ❖ Parametrii

# Funcții Specifice în C

❖ `printf`: Scrie formatat la stdout.

# Funcții Specifice în C

- ❖ `printf`: Scrie formatat la `stdout`.
- ❖ `fprintf`: Scrie formatat într-un fișier.

# Funcții Specifice în C

- ❖ `printf`: Scrie formatat la `stdout`.
- ❖ `fprintf`: Scrie formatat într-un fișier.
- ❖ `sprintf`: Scrie formatat într-un șir de caractere.

# Funcții Specifice în C

- ❖ `printf`: Scrie formatat la `stdout`.
- ❖ `fprintf`: Scrie formatat într-un fișier.
- ❖ `sprintf`: Scrie formatat într-un șir de caractere.
- ❖ `snprintf`: Scrie formatat într-un șir de caractere, ținând cont și de lungimea maximă.



# Șiruri de Caractere de Formatare. Parametrii

# Șiruri de Caractere de Formatare. Parametrii

- ❖ **Șiruri de Caractere de Formatare:** Șir de caractere format din text propriu-zis (ce va fi scris ca atare) și din parametrii (identificați prin %)

# Șiruri de Caractere de Formatare. Parametrii

- ❖ **Șiruri de Caractere de Formatare:** Șir de caractere format din text propriu-zis (ce va fi scris ca atare) și din parametrii (identificați prin %)
- ❖ Exemple de parametrii

# Șiruri de Caractere de Formatare. Parametrii

- ❖ **Șiruri de Caractere de Formatare:** Șir de caractere format din text propriu-zis (ce va fi scris ca atare) și din parametrii (identificați prin %)
- ❖ Exemple de parametrii
  - ❖ **d:** Scrie în format zecimal valoarea primită ca parametru.

# Șiruri de Caractere de Formatare. Parametrii

- ❖ **Șiruri de Caractere de Formatare:** Șir de caractere format din text propriu-zis (ce va fi scris ca atare) și din parametrii (identificați prin %)
- ❖ Exemple de parametrii
  - ❖ **d:** Scrie în format zecimal valoarea primită ca parametru.
  - ❖ **x:** Scrie în format hexazecimal valoarea primită ca parametru.

# Șiruri de Caractere de Formatare. Parametrii

- ❖ **Șiruri de Caractere de Formatare:** Șir de caractere format din text propriu-zis (ce va fi scris ca atare) și din parametrii (identificați prin %)
- ❖ Exemple de parametrii
  - ❖ **d:** Scrie în format zecimal valoarea primită ca parametru.
  - ❖ **x:** Scrie în format hexazecimal valoarea primită ca parametru.
  - ❖ **s:** Dereferențiază adresa primită ca parametru și scrie șirul de caractere (terminat în NULL) găsit acolo.

# Șiruri de Caractere de Formatare. Parametrii

- ❖ **Șiruri de Caractere de Formatare:** Șir de caractere format din text propriu-zis (ce va fi scris ca atare) și din parametrii (identificați prin %)
- ❖ Exemple de parametrii
  - ❖ **d:** Scrie în format zecimal valoarea primită ca parametru.
  - ❖ **x:** Scrie în format hexazecimal valoarea primită ca parametru.
  - ❖ **s:** Dereferențiază adresa primită ca parametru și scrie șirul de caractere (terminat în NULL) găsit acolo.
  - ❖ **n:** Populează o zonă de memorie primită ca parametru cu numărul de caractere ce au fost scrise.

# Atacuri cu Șiruri de Caractere de Formatare



- ❖ Presupun injectarea unui astfel de șir de caractere într-o funcție.

# Atacuri cu Șiruri de Caractere de Formatare

- ❖ Presupun injectarea unui astfel de șir de caractere într-o funcție.
- ❖ Asemănător injectării în șabloane la nivel de server (engl. "*server-side template injection*" și abreviat SSTI)

# Rezultatele Atacurilor

- Citirea informației din memoria procesului

- Citirea informației din memoria procesului
- Modificarea informației din memoria procesului

# Protecții împotriva Atacurilor

- Sanitizarea intrărilor de la utilizator

# Protecții împotriva Atacurilor

- ❖ Sanitizarea intrărilor de la utilizator
- ❖ Activarea avertizărilor și a protecțiilor, la nivel de compilator



# Exerciții



- ❖ Folosiți comanda `man` pentru a primi ajutor la rularea anumitor comenzi.

- ❖ Folosiți comanda `man` pentru a primi ajutor la rularea anumitor comenzi.
- ❖ Folosiți documentația `pwntools` pentru a identifica metodele de care aveți nevoie.

# ***Exemplu Concret***

# Atacuri în Sistemele Multimedia ale Mașinilor I

# Atacuri în Sistemele Multimedia ale Mașinilor I



# Atacuri în Sistemele Multimedia ale Mașinilor II



# Atacuri în Sistemele Multimedia ale Mașinilor II

- Multiple vulnerabilități la atacuri cu șiruri de caractere de formatare, găsite în sistemele multimedia ale unor mașini

# Atacuri în Sistemele Multimedia ale Mașinilor II

- ❖ Multiple vulnerabilități la atacuri cu șiruri de caractere de formatare, găsite în sistemele multimedia ale unor mașini
- ❖ Numele dispozitivului conectat ca vector de atac

# Atacuri în Sistemele Multimedia ale Mașinilor II

- ❖ Multiple vulnerabilități la atacuri cu șiruri de caractere de formatare, găsite în sistemele multimedia ale unor mașini
- ❖ Numele dispozitivului conectat ca vector de atac
- ❖ Mai multe mașini găsite ca fiind vulnerabile ca urmare a unei postări inițiale pe Twitter

# Atacuri în Sistemele Multimedia ale Mașinilor II

- ❖ Multiple vulnerabilități la atacuri cu șiruri de caractere de formatare, găsite în sistemele multimedia ale unor mașini
- ❖ Numele dispozitivului conectat ca vector de atac
- ❖ Mai multe mașini găsite ca fiind vulnerabile ca urmare a unei postări inițiale pe Twitter
  - ❖ BMW 330i 2011

# Atacuri în Sistemele Multimedia ale Mașinilor II

- ❖ Multiple vulnerabilități la atacuri cu șiruri de caractere de formatare, găsite în sistemele multimedia ale unor mașini
- ❖ Numele dispozitivului conectat ca vector de atac
- ❖ Mai multe mașini găsite ca fiind vulnerabile ca urmare a unei postări inițiale pe Twitter
  - ❖ BMW 330i 2011
  - ❖ Camioane GMC 2016

# Atacuri în Sistemele Multimedia ale Mașinilor II

- ❖ Multiple vulnerabilități la atacuri cu șiruri de caractere de formatare, găsite în sistemele multimedia ale unor mașini
- ❖ Numele dispozitivului conectat ca vector de atac
- ❖ Mai multe mașini găsite ca fiind vulnerabile ca urmare a unei postări inițiale pe Twitter
  - ❖ BMW 330i 2011
  - ❖ Camioane GMC 2016
  - ❖ Audi A7 2014

# Recapitulare

# Recapitulare



# Recapitulare

