TU Wien
Institut für Information Systems Engineering
Forschungsgruppe Industrial Software
Arbeitsgruppe ESSE
https://security.inso.tuwien.ac.at/

Abgabedokument Lab1

Introduction to Security

183.594 – WS 2018

27.11.2018

Team 48

Name	**MatrNr.**
Tristan Ulreich	01326158
Martha Musterfrau	1234567
Otto Mustermann	0815421
Otto Mustermann	0995421
Otto Mustermann	0236214

Inhaltsverzeichnis

1 Ueberschrift 1

1.1 Hinweise

Hinweise:

- Verwenden sie entweder diese deutsche Version oder die englische Version in `protocol.tex`
- Setzen sie alle Variablen nach *FOR STUDENTS* in der .tex Datei
- Ersetzen sie die Platzhalter für ihre Namen und MatNr.
- Löschen sie diese Sektion über Hinweise und die folgenden Beispiel-Kapitel
- Achten sie auf geforderte Formate und Anforderungen an die Dateinamen
- Führen Sie `pdflatex` mindestens 2 mal aus, damit die Referenzen und Seitenzahlen richtig im PDF dargestellt werden
- Sie koenen dazu auch das Makefile verwenden: `make de`

1.2 Sub-Ueberschrift 1

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

1.3 Sub-Ueberschrift 2

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

2 Forensik

2.1 Lizenzvertrag

Um diese Aufgabe bearbeiten zu können, muss man zuerst das PDF erlangen. Dazu habe ich mir die Datei in /ssh/config angelegt mit folgenden Daten:

Host lab
HostName tese.inso.tuwien.ac.at
Port 12345
User e01326158

Anschließend habe ich im Terminal den Befehl ssh -L 8048:10.10.10.100:8048 lab ausgeführt und somit eine SSH-Portweiterleitung instanziert. Um nun das PDF herunterzuladen habe ich im Browser

$localhost : 8048/downloads/Vertragsunterlagen_vertraulich.pdf$

eingegeben um das PDF herunterzuladen. Im Anschluss habe ich einfach den ausgeschwärzten Text im PDF markiert und somit die "geschwärzteSZahl herausfinden können.

1.804.167.212

2.2 Lizenz-Nachzahlung

Um die Lizennachzahlung heruaszufinden, habe ich auf den ausgegrauten Text herangezoomt und festgestellt, dass die ursprüngliche Zahl noch leicht sichtbar ist. Ich hätte auch den Kontrast des PDF-Ausschnittes ändern können um den Preis sichtbarer zu machen.

7.716.465.296

2.3 Crypto-Ref-ID

Die Crypto-Ref-ID steht in den Eigenschaften des PDF Dokumentes.

$A13m7X07$

2.4 Lizenz Berechtigung

Die Zahlungsreferenz ist abseits des sichtbaren (für den PDF-Reader) PDFs gespeichert.

$RE151 - 774 - T - 31$

2.5 Appendix 07

Ich habe das PDF in LibreOffice-Draw geöffnet (PDF-Editor). Hinter dem Bild ist ein zweites wesentlich kleineres Bild gespeichert, mit der Zeit.

$08 : 58 : 87$

3 Manager9000

3.1 Schwachstelle finden

Die Seite ist SQL Injection gefährdet. Mit dem Eingabedaten $'OR'1' =' 1'--$ in Nickname und Passwort kann fälschlicherweise eingeloggt werden.

3.2 Wer schürft am meisten?

Mittels $'OR'1' =' 1');droptableid$ kann die gesamte Liste der Miner ausgegeben werden, da bei Syntaxfehlern der ausgeführte SQL-Code ausgegeben wird, kann hier einfach die Eingabe angepasst werden. Nun muss nur noch der/die stärkste/er herausgesucht werden.

3.3 Mein Wallet

SELECT id, name, phone, country, city, street, number FROM contacts WHERE (name LIKE '% 'OR '1'='1'); SELECT id, name, phone, country, city, street, number FROM contacts ORDER BY name ; (' %')

4 Beispiele

4.1 Source Code formatieren

Es folgen einige Beispiele wie Sourcecode in diesem Dokument formatiert und referenziert werden kann (siehe Listing 1 auf Seite 5 und siehe Listing 2 auf Seite 5).

Ebenso können kurzer Code oder kurze Befehle direkt in der Zeile in einem `lstinline Block` mit typengleicher Schrift formatiert werden.

```
/*
 * Just an example C-file.
 */

#include <stdio.h>

int global_variable = 1;
#ifdef DEBUG
int another_global_variable = 1;
#endif

/*
 * Some comment
 */
int main(void)
{
  temp_variable = 4711;
  another_variable = 0815;

  printf("foo bar baz %02d", temp_variable);

  return 1;
}
```

Listing 1: Example C/C++ file

```
#!/bin/bash
echo "Bash version ${BASH_VERSION}..."
for i in {0..10..2}
  do
     echo "Welcome $i times"
 done
```

```
8 echo "some very very very very very very very very very ↵
    very very very very very very very very very very very ↵
    long string"

10 exit 0;
```

Listing 2: Example bash script

4.2 Bilder

Es folgen einige Beispiele wie Bilder in diesem Dokument eingefuegt werden koennen (siehe Abbildung 1 auf Seite 6).

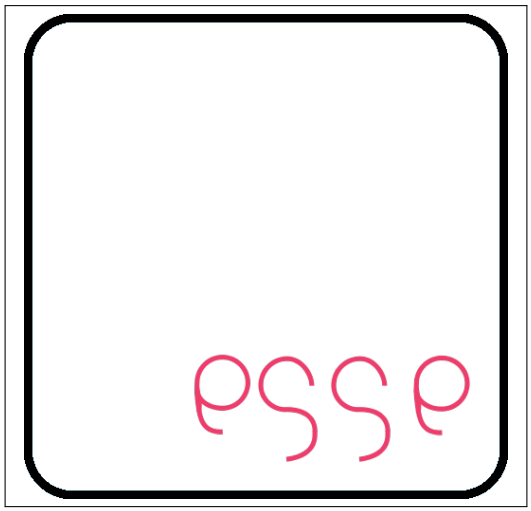

Abbildung 1: ESSE Logo