TU Wien
Institut für Information Systems Engineering
Forschungsgruppe Industrial Software
Arbeitsgruppe ESSE
https://establishing-security.at/

Abgabedokument Lab1

Einführung in Security

194.157 – 2024 W

16. Dezember 2024

Team 44

Name	**MatrNr.**
Kevin Csele	12122544
Clemens Schneider	MATRIKELNUMMER
Luka Twaroch	MATRIKELNUMMER
Wen Long Zhou	MATRIKELNUMMER
Ramin Shaikh	12123657

Inhaltsverzeichnis

HINWEIS

Bitte halten Sie sich genau an die Struktur im jCTF. Bitte beginnen Sie mit der ersten Kategorie, d.h., “Der Service war auch schon besser ...” und den entsprechenden Unteraufgaben. Bitte gehen Sie immer von links nach rechts und von oben nach unten vor. Eine Kategorie ist eine section, eine Challenge eine subsection. Bitte erstellen Sie auch Einträge für Beispiele, die Sie nicht gelöst haben. (Diesen HINWEIS gerne löschen!)

1 Der Service war auch schon besser ...

1.1 Achtung! Streng geheim!

Nicht gelöst.

1.2 Eine schräge Nummer

Nicht gelöst.

1.3 Was letzte Preis?

Nicht gelöst.

1.4 IBANs sollte man verbannen!

Nicht gelöst.

2 Cäsars Schlüsselbund

2.1 Schlüssel. Knacken.

Nicht gelöst.

2.2 Passwörter Retten.

Nicht gelöst.

3 Paranoider Mozart

3.1 MozART.

Nicht gelöst.

4 Zertifiziertes Durcheinander

4.1 Zertifizieren ist schwer

Um den Certificate Signing Request zu erstellen habe ich den folgenden Befehl verwendet: `openssl req -newkey rsa:4096 -sha512 -config openssl.cnf -out csr.csr -subj "/CN=12123657-Intermediate-CA-WS2024/OU=ESSE-Lab1-Exercise"`
`req` ist der Befehl um einen CSR zu erstellen;
`-newkey rsa:4096` spezifiziert, dass ein neuer Key (4096-Bit RSA) erstellt werden soll;
`-sha512` gibt an, dass sha512WithRSAEncription als Signaturalgorithmus verwendet werden soll;
mit `-config` wird angegeben, welches config file zu verwenden ist;
`-out` bestimmt das output-file und
`-subj "/CN=12123657-Intermediate-CA-WS2024/OU=ESSE-Lab1-Exercise"` definiert die gewünschten Namens-Parameter im CSR.

Das config file dient dazu, die nötigen X509v3 Parameter zu setzen und sieht aus wie folgt:

```
[ req ]
default_bits            = 4096
default_md              = sha512
default_keyfile         = privkey.pem
distinguished_name      = req_distinguished_name
req_extensions           = v3_req

[ req_distinguished_name ]

[ v3_req ]
subjectKeyIdentifier = hash
basicConstraints = critical, CA:true, pathlen:0
keyUsage = critical, Certificate Sign, CRL Sign
```

Listing 1: openssl.cnf

Nach Ausführung des oben genannten Befehls, wird der CSR in der Datei csr.csr gespeichert, diese wurde im Abgabetool eingereicht.

5 Zeitreise durch das World Wide Web

5.1 Wieder Elvis

Nicht gelöst.

5.2 CäsarMussWeg! MussCäsarWeg?

Nicht gelöst.

5.3 dackboor.

Nicht gelöst.

5.4 Schlechtes Timing (Time Travel Edition)

Nicht gelöst.

5.5 Sorcerer ... ?

Nicht gelöst.

6 Seitlich fließend

6.1 Newton und Co KG.

Nicht gelöst.

7 Antike Mobile Security

7.1 iTimeTravel

Nicht gelöst.

7.2 AND(roid)ERS

Nicht gelöst.

8 Babycam Espionage

8.1 The Rise of the HuManoiD5

Nicht gelöst.

8.2 ETA

Nicht gelöst.

9 Das Social Media der Zukunft

9.1 Der vergiftete Passwort Reset

Nicht gelöst.

9.2 Accountübernahme

Nicht gelöst.

10 Hidden Timelines

10.1 Phantom Domain

Nicht gelöst.

11 Vault Voyage

11.1 That's all your vault!

Nicht gelöst.

12 Wikinger Overflow

12.1 Überlauf. Hand drauf.

Nicht gelöst.

12.2 Typisch Typing ... Stufe 1

Nicht gelöst.

12.3 Typisch Typing ... Stufe 2

Nicht gelöst.

12.4 Typisch Typing ... Stufe 3

Nicht gelöst.

13 Tap to the Future

13.1 Tick Tock Tap

Nicht gelöst.

14 So viele

14.1 Das Device ist heiß

Nicht gelöst.

14.2 Persona non grata

Nicht gelöst.

14.3 Eine Frage der Kommunikation

Nicht gelöst.

14.4 Treffpunkt

Nicht gelöst.

14.5 Alles dokumentiert!

Nicht gelöst.

14.6 Es geht immer um Inhalte

Nicht gelöst.

15 Web of Treats

Nicht gelöst.

15.1 Mitgliedschaftsnr.

Nicht gelöst.

15.2 Geheimer Artikel

Nicht gelöst.

15.3 Überfüllt

Nicht gelöst.

15.4 A shell in the forest?

Nicht gelöst.

15.5 Elvis

Nicht gelöst.

16 Das. Beste. Text. Adventure. Aller. Zeiten.

16.1 Time to travel!

Nicht gelöst.

16.2 Mein Name?

Nicht gelöst.

16.3 Ein PIN!

Nicht gelöst.

16.4 Ach ... ein Schlüssel

Nicht gelöst.

16.5 Flag!

Nicht gelöst.

17 Passwörter werden wir auch nie los, oder?!

17.1 Gute Idee, um ein Passwort zu verstecken?!

Nicht gelöst.

17.2 Call Julius ... äh. John.

Nicht gelöst.

17.3 Nicht nur Ziffern, sonder auch ...?

Nicht gelöst.

17.4 /etc/ANTIK?

Nicht gelöst.

17.5 Sicher sicher?

Nicht gelöst.

17.6 Zeitlose Liste

Nicht gelöst.

17.7 (Image)magic(k)

Nicht gelöst.

17.8 Auch in Zukunft ein schweres Passwort?

Nicht gelöst.

18 Franz Joseph und die Kommandozeile

18.1 Stage

Nicht gelöst.

18.2 Stagee

Nicht gelöst.

18.3 Stageee

Nicht gelöst.

18.4 Stageeee

Nicht gelöst.

18.5 Stageeeee

Nicht gelöst.

18.6 Stageeeeee

Nicht gelöst.

18.7 Stageeeeeee

Nicht gelöst.

18.8 Stageeeeeeee

Nicht gelöst.

18.9 Stageeeeeeeee

Nicht gelöst.

18.10 Stageeeeeeeeee

Nicht gelöst.

18.11 Stageeeeeeeeeee

Nicht gelöst.

18.12 Stageeeeeeeeeeee

Nicht gelöst.

19 Bot Bot Bot Bot

19.1 I keep you my little secret ...

Nicht gelöst.

20 Wireless Time Travel

20.1 Vir zukunftssichere Handschläge

Nicht gelöst.

20.2 Code der Zukunft

Nicht gelöst.

20.3 Ungewöhnlich verschlüsselte Botschaft

Nicht gelöst.

20.4 Geheimnisvoller Zugang: superboss

Nicht gelöst.

20.5 Unbrauchbarer Schlüssel

Nicht gelöst.

20.6 Einen Schlüssel für einen Schlüssel! Echt jetzt?!

Nicht gelöst.

20.7 Verborgenes Protokoll

Nicht gelöst.

21 Ueberschrift 1

21.1 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 zweimal aus, damit die Referenzen und Seitenzahlen richtig im PDF dargestellt werden.
- Sie können dazu auch das Makefile verwenden: `make de`.

22 Beispiele

22.1 Source Code formatieren

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

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

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

echo "some very very very very very very very very very very
   very very very very very very very very very very very very
   long string"

exit 0;
```

Listing 3: Example bash script

22.2 Bilder

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

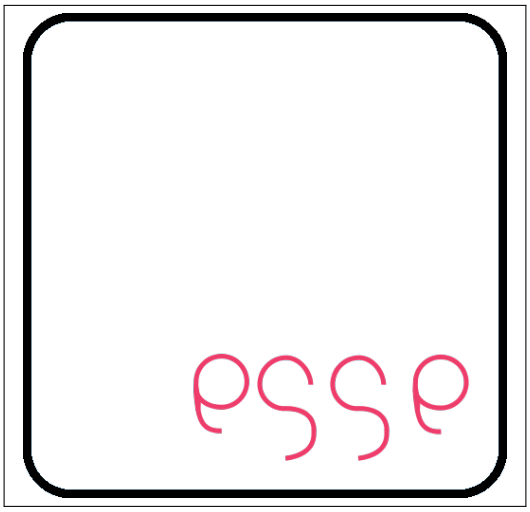

Abbildung 1: ESSE Logo

```c
/*
 * 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 2: Example C/C++ file