IISC/CTF: replme

Review of TestCTF#1

Jacob Bachmann

SecT
TU Berlin

January 1, 1980

About service: replme

About service: replme

”many dockers”
– henning –

About service: replme

- Provides temporary REPLs

About service: replme

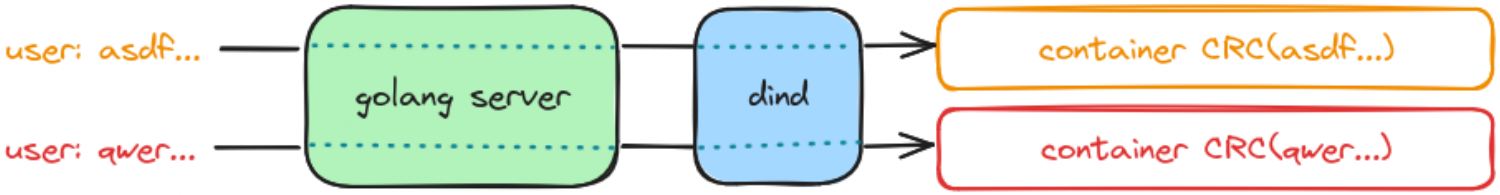
- Provides temporary REPLs
- Soon™ implements temp Devenvs à la replit.com

About service: replme

- Provides temporary REPLs
- Soon™ implements temp Devenvs à la replit.com
- Vuln#1: Exploit through second pre-image attack

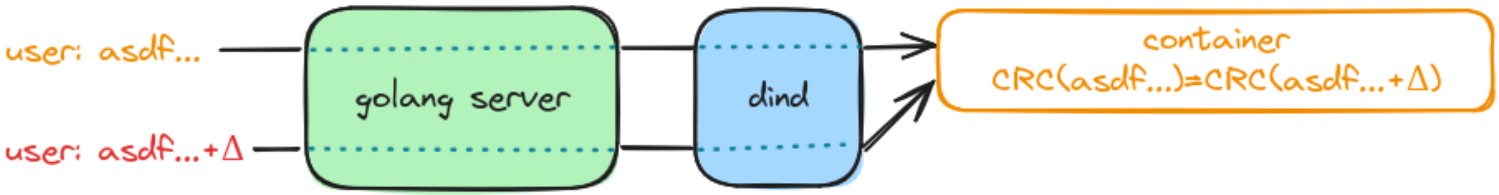
About service: replme

- Provides temporary REPLs
- Soon™ implements temp Devenvs à la replit.com
- Vuln#1: Exploit through second pre-image attack



About service: replme

- Provides temporary REPLs
- Soon™ implements temp Devenvs à la replit.com
- Vuln#1: Exploit through second pre-image attack



What works?


SECURITY IN TELECOMMUNICATIONS
SECT
TECHNISCHE UNIVERSITÄT BERLIN

What works?

Service

- Stability: No crashes, no unexpected behaviour
- Cleanup: Garbage collected
- Security: No unintended vulns have been found

What works?

Service

- Stability: No crashes, no unexpected behaviour
- Cleanup: Garbage collected
- Security: No unintended vulns have been found

Checker

- Stability: Mostly (later more)
  - put/getflag stable
  - put/getnoise mostly stable
  - havoc stable
- Functionality: Detected dead services as intended

What works?

Service

- Stability: No crashes, no unexpected behaviour
- Cleanup: Garbage collected
- Security: No unintended vulns have been found

Checker

- Stability: Mostly (later more)
  - put/getflag stable
  - put/getnoise mostly stable
  - havoc stable
- Functionality: Detected dead services as intended

Fix

- Worked locally (more details later)

What works?

Feedback Christian

- Vuln: Medium+ to hard difficulty
- Codebase: Large with much to look through

What doesn't?


SECURITY IN TELECOMMUNICATIONS
SECT
TECHNISCHE UNIVERSITÄT BERLIN

What doesn't?

Service

- Henning: Welcome page says "cafedodo"

What doesn't?

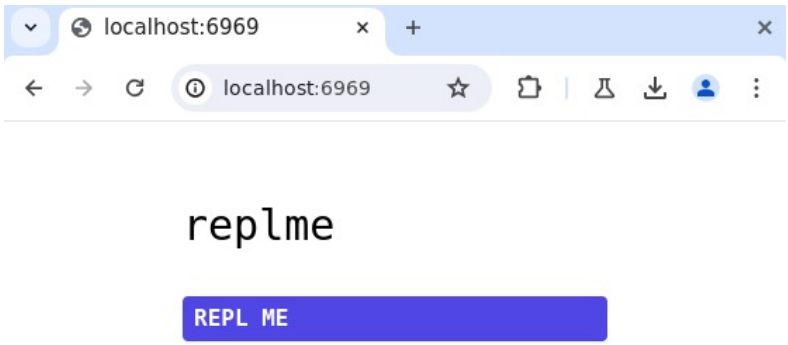
Service

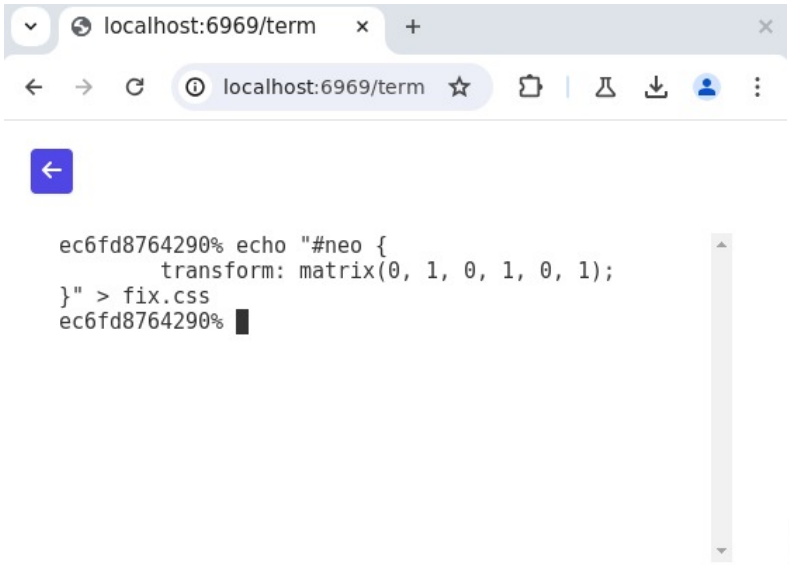
- Henning: Welcome page says "cafedodo"
- M[o]aath: Needs CSS treatment

What doesn’t?

Service

- Henning: Welcome page says ”cafedodo”
- M[o]aath: Needs CSS treatment





What doesn’t?

Service

- Henning: Welcome page says ”cafedodo”
- M[o]aath: Needs CSS treatment
- M[o]aath: Idea with server unclear

What doesn't?

Service

- Henning: Welcome page says "cafedodo"
- M[o]aath: Needs CSS treatment
- M[o]aath: Idea with server unclear
- Service rebuild failed due to IP blacklisting
  - $\Rightarrow$ Adjust Dockerfile

What doesn't?

Service

- Henning: Welcome page says "cafedodo"
- M[o]aath: Needs CSS treatment
- M[o]aath: Idea with server unclear
- Service rebuild failed due to IP blacklisting
  - $\Rightarrow$ Adjust Dockerfile

Checker

- Putnoise sometimes timed out

What doesn't?

Service

- Henning: Welcome page says "cafedodo"
- M[o]aath: Needs CSS treatment
- M[o]aath: Idea with server unclear
- Service rebuild failed due to IP blacklisting
  - $\Rightarrow$ Adjust Dockerfile

Checker

- Putnoise sometimes timed out
- No information in chaindb

What doesn't?

Service

- Henning: Welcome page says "cafedodo"
- M[o]aath: Needs CSS treatment
- M[o]aath: Idea with server unclear
- Service rebuild failed due to IP blacklisting
  - $\Rightarrow$ Adjust Dockerfile

Checker

- Putnoise sometimes timed out
- No information in chaindb
- Getnoise can't retrieve chaindb info
  $\Rightarrow$ exception

What doesn't?

Service

- Henning: Welcome page says "cafedodo"
- M[o]aath: Needs CSS treatment
- M[o]aath: Idea with server unclear
- Service rebuild failed due to IP blacklisting
  - ⇒ Adjust Dockerfile

Checker

- Putnoise sometimes timed out
- No information in chaindb
- Getnoise can't retrieve chaindb info
  ⇒ exception
  - ⇒ Tweak timeouts (Munchkin: 2.6s)

What doesn't?

Service

- Henning: Welcome page says "cafedodo"
- M[o]aath: Needs CSS treatment
- M[o]aath: Idea with server unclear
- Service rebuild failed due to IP blacklisting
  - ⇒ Adjust Dockerfile

Checker

- Putnoise sometimes timed out
- No information in chaindb
- Getnoise can't retrieve chaindb info
  ⇒ exception
  - ⇒ Tweak timeouts (Munchkin: 2.6s)
  - ⇒ Wrap chaindb calls in try+catch

Miscellaneous

Miscellaneous

- Dind can be RAM killer when not GCed
- Players could DOS contrahent service by opening many sessions without killing
- $\Rightarrow$ Node.js server consumes >60MB RAM
  $\Rightarrow$ Rewrite in 🦀
- $\Rightarrow$ Player sessions need to be monitored
  $\Rightarrow$ Malicious behaviour leads to ban

Lessons learned

Lessons learned

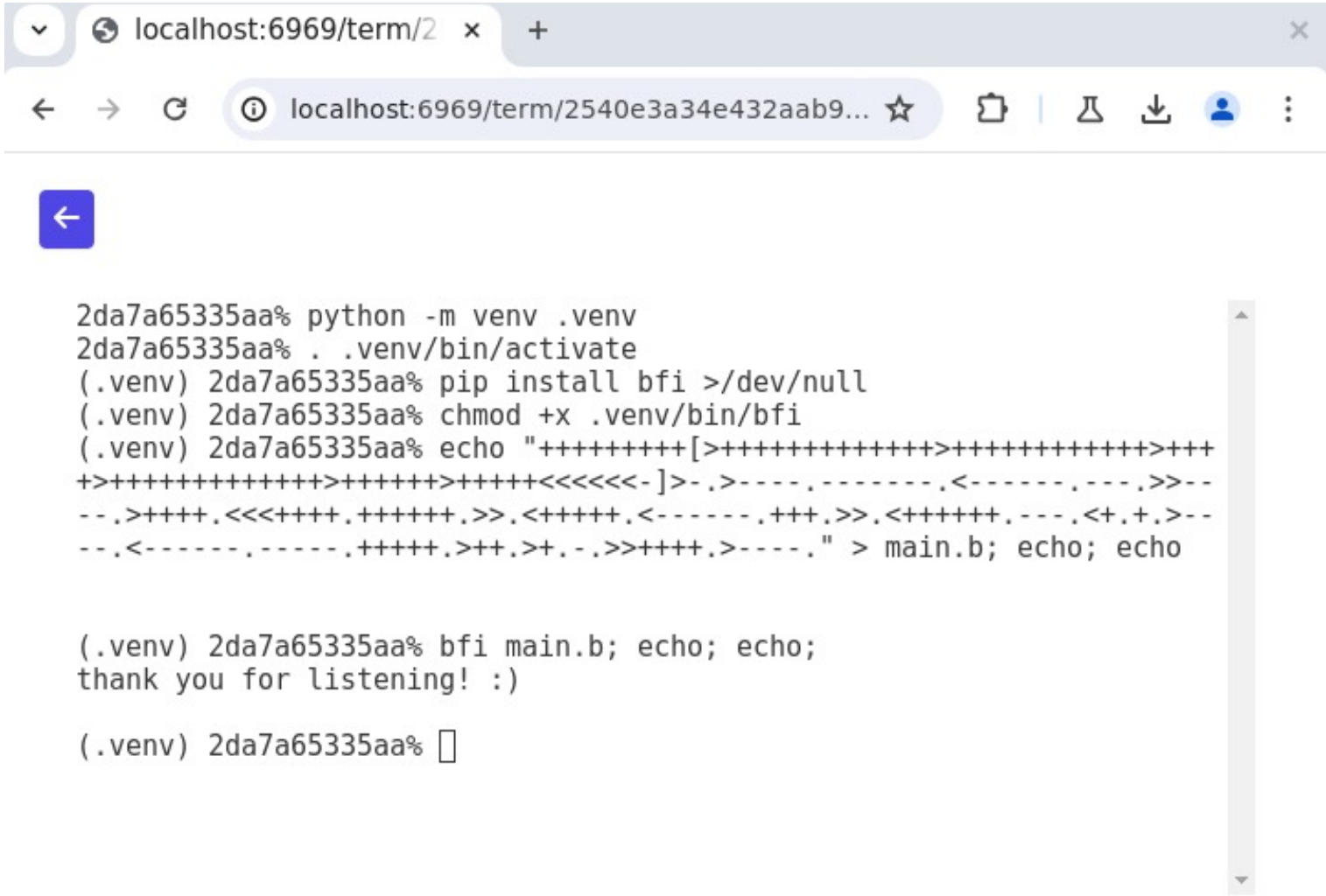
- More stress testing, e.g.
  VM w/ low core and RAM amount + x times traffic

Lessons learned

- More stress testing, e.g.
  VM w/ low core and RAM amount + x times traffic
- Don't get caught in details, your CSS will suffer from it

Lessons learned

- More stress testing, e.g.
  VM w/ low core and RAM amount + x times traffic
- Don't get caught in details, your CSS will suffer from it
- Design Dockerfiles for chachable layer support


localhost:6969/term/2
localhost:6969/term/2540e3a34e432aab9...
2da7a65335aa% python -m venv .venv
2da7a65335aa% . .venv/bin/activate
(.venv) 2da7a65335aa% pip install bfi >/dev/null
(.venv) 2da7a65335aa% chmod +x .venv/bin/bfi
(.venv) 2da7a65335aa% echo "+++++++++[>++++++++++++++>++++++++++++>+++
+>++++++++++++>++++++>+++++<<<<<<-]>-.>----.--------.<------.---.>>--
--.>++++.<<<++++.++++++.>>.<+++++.<------.+++.>>.<++++++.---.<+.+.>--
--.<------.-----.+++++.>++.>+.-.>>++++.>----." > main.b; echo; echo
(.venv) 2da7a65335aa% bfi main.b; echo; echo;
thank you for listening! :)
(.venv) 2da7a65335aa%