BUG HUNTING PRAKTIKUM

Praktikum Kick-Off

Fraunhofer

(Security-)

BUGS

EGAL

Denial of Service

Broken Authentication

Memory Corruption

XSS

Denial of Service

SQL Injection

Und viele mehr!

„Open Source“

- github.com, gitlab.com, …
- Bekannter Projekte (>50 Sterne, andere Metrik, …)

Kommerzielle Programme

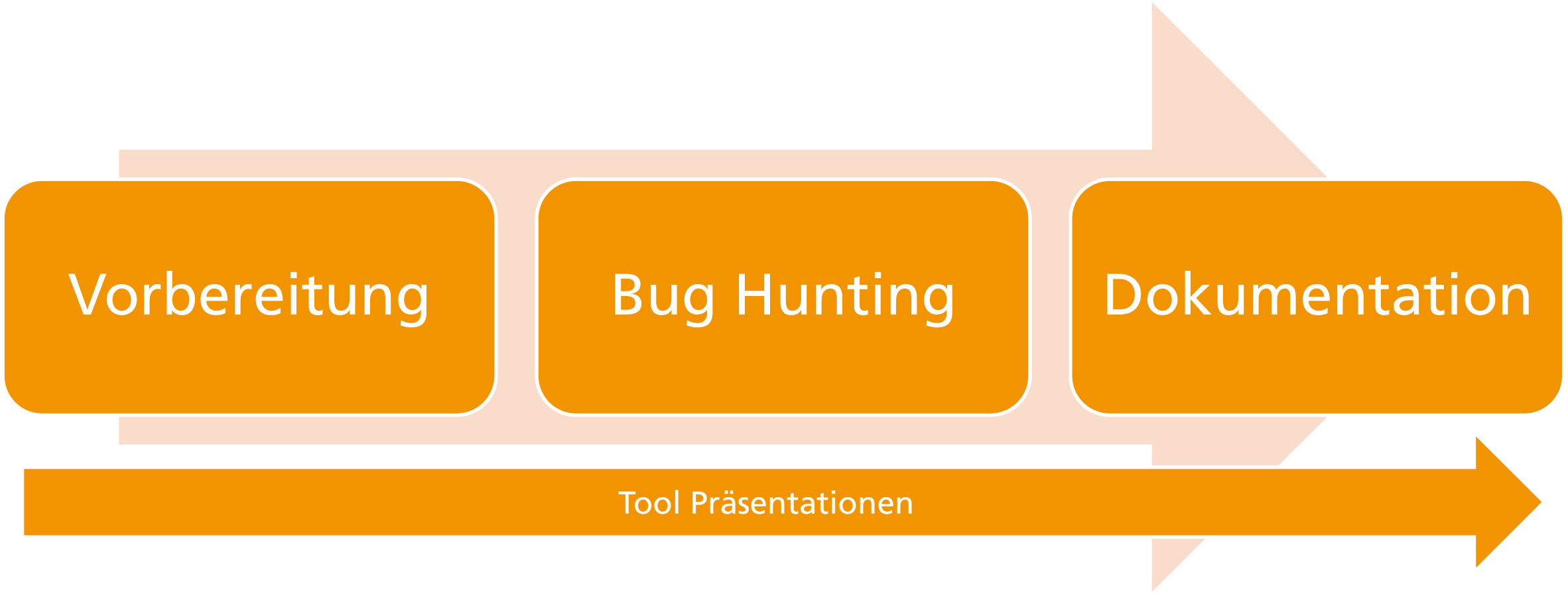
- In der Regel kein Source Code
- Gemeinschaftsgedanke?
- Kostenloses Pentesten?

- Fraunhofer SIT – Institut für sichere Informationstechnologie
- Abteilung SSE – Secure Software Engineering
- Analyse von Binaries, Penetration Tests, Code Reviews, Bedrohungsmodellierung
  - Philipp Roskosch
  - Sebald Ziegler
  - Michael Tröger

Organisatorisches – 2er Gruppen

https://i.imgur.com/66t9tvT.gifv

Phasen



Phase 1 – Vorbereitung

3 Rubriken

- PHP Webshops
- Android E-Mail Clients
- Linux Multimedia Player

Pro Rubrik

- Mindestens 3 Targets heraussuchen + ausprobieren
- Angriffsziele
- Voraussetzungen
- Mindestens 2 Angreifer modellieren
- Attack Surfaces
- Vorgehen

Rubrik: Android Password Manager

- Targets:
  - KeePassX
  - Bitwarden
  - Buttercup
- Angriffsziele:
  - Passwörter stehlen
  - Master Passwort stehlen
  - Mail-Adressen/Domains/Usernames stehlen
- Voraussetzungen:
  - Android Smartphone

Phase 1 – Mini Mini Mini Beispiel Angreifer

Taschendieb

- Angreifer hat Smartphone gestohlen
- Es ist unlocked
- Nicht unendlich Rechenpower

Mitarbeiter

- Angreifer ist Mitarbeiter beim Passwort Manager
- Zugriff auf alle synchronisierten Daten

Phase 1 – Mini Mini Mini Beispiel Attack Surface

Datenbank

Convenience Funktionen

Masterpasswort Eingabe

Netzwerk Verkehr

Phase 1 – Mini Mini Mini Beispiel Vorgehen

Datenbank Speicherung prüfen

Verschlüsselung der Datenbank prüfen

Netzwerk Verkehr prüfen

Phase 1 – Mini Mini Mini Beispiel Abschätzung

Gibt es genug zu tun?

Schwierige Voraussetzungen?

Phase 1 – Deliverables

PDF Report

- Ausarbeitung der Rubriken
- Keine Stichpunkte
- Handwerkszeug nächste Woche

Präsentation der Ergebnisse

- Slides
- 5-10 Minuten
- Ende Phase 1

Phase 2 – Bug Hunting

BUGS suchen

- In Targets aus Phase 1

BUGS melden

- Sofort melden an bughunting@sit.fraunhofer.de mit Template
- Wir melden an Hersteller/Entwickler
- Duplicates werden abgelehnt

BUGS vorstellen

- In den Treffen
- Relativ kurz
- Keine vorgegebene Form

Phase 2 – Bug Hunting

Kann passieren	Sollte passieren	Muss passieren
Plan ändern	**Dokumentieren**	**Tool Präsentationen**
• Targetliste erweitern • neue Rubrik hinzufügen • Neue Angreifermodelle, etc.	• Alle (!) Tests, auch ohne Befund • Ergebnisse • Skripte/Commands • SCREENSHOTS, SCREENSHOTS, SCREENSHOTS	• während dieser Phase

Nebenbei: Tool Präsentationen

- Vortrag über ein Hacking Tool
- Exakt 15 Minuten
- Z.B. sqlmap, angr, ida, ghidra, ZAP, burp, …
- Anwendungsfall
- Usage
- Funktionsweise
- Interessantere Features!!!
- Demo Time

Ein Wort zu Bug Bounties

hackerone

zerodium

bugcrowd

- Wir sind verpflichtet, Bugs zu melden, wenn wir davon erfahren
- Euch Bounties auszuzahlen, ist organisatorisch sehr schwierig

oder

https://aford.be/wp-content/uploads/2019/01/ECTS.jpg
https://www.hackerone.com/assets/images/logo.png
https://www.asmgi.com/wp-content/uploads/2018/01/download.jpg
https://itcurated.com/infosecindex/wp-content/uploads/sites/35/2017/02/zerodium-cybersecurity.jpg
https://timedotcom.files.wordpress.com/2017/08/money-dirty-hands-microbes.jpg?quality=85&w=1012&h=569&crop=1

Phase 3 - Dokumentation

Bugs melden nicht mehr möglich

Report abgabebereit machen

- Alle Ergebnisse und Tests ausarbeiten
- Einleitung/Abschluss schreiben

Termine

SPRECHSTUNDEN VORHER KURZ ANMELDEN AN bughunting@sit.fraunhofer.de

Datum		
16.10	DIESE WOCHE	Phase 1
23.10	Kleine Bug Hunting Intro	
30.10	-	
06.11	Sprechstunde	
13.11	Phase 1 Abschluss (5 Min. Präsentation) **PRÜFUNGSRELEVANT**	
20.11	Sprechstunde	Phase 2
27.11	2 Präsentationen **PRÜFUNGSRELEVANT**	
04.12	Sprechstunde	
11.12	2 Präsentationen **PRÜFUNGSRELEVANT**	
18.12	*„Fällt Aus“*	
25.12	WEIHNACHTSFERIEN	
01.01	WEIHNACHTSFERIEN	

Termine

Datum		
08.01	WEIHNACHTSFERIEN	Phase 2
15.01	2 Präsentationen **PRÜFUNGSRELEVANT**	
22.01	Sprechstunde	
29.01	1 Präsentation **PRÜFUNGSRELEVANT**	
05.02	Sprechstunde	
12.02	Phase 2 endet – Abschlusstermin!!! Letzte Vorlesungswoche	
19.02	Sprechstunde	Phase 3
26.02	Sprechstunde	
04.03	Sprechstunde	
08.03	23:59 Finale REPORT ABGABE!!!!1!!11 **PRÜFUNGSRELEVANT**	
31.03	Semesterende	

TeamSIK Space

- TeamSIK trifft sich mittwochs 18:00
- Ihr seid herzlich eingeladen
- Platz für Bug Hunting Praktikum/TeamSIK
- Keine Sprechstunde, keine Betreuung
- Free Food
- Sagt Bescheid, wenn ihr Bock habt an bughunting@sit.fraunhofer.de
- Zugangsvertrag

Was ist, wenn man keine Bugs findet?

- Präsentationen
- Qualität des Reports
- Befundlose Tests gut dokumentieren
- Strukturierte Vorgehensweise
- Kann auch noch zu guter Note führen!

FRAGEN?

Fraunhofer

TEAM UND TOOL SUCHE!!!

- Beispiel Tools
  - Sqlmap
  - Metasploit
  - Gdb
  - Frida
  - angr
  - ghidra
  - ZAP
  - AFL
  - pwntools

- Termine
  - 27.11 2 Slots
  - 11.12 2 Slots
  - 15.01 2 Slots
  - 29.01 2 Slots

Sonst?

- Bei TuCAN anmelden
- Fragen immer an bughunting@sit.fraunhofer.de
- Informationen auch unter https://team-sik.org/bug-hunting-praktikum/

Phase 1 beginnt