DIHSÜD

FH | JOANNEUM
University of Applied Sciences

ETHICAL HACKING
Penetration Testing vs. Bug Bounty Programme

Dr. KL@U5 Ge8eSHuber

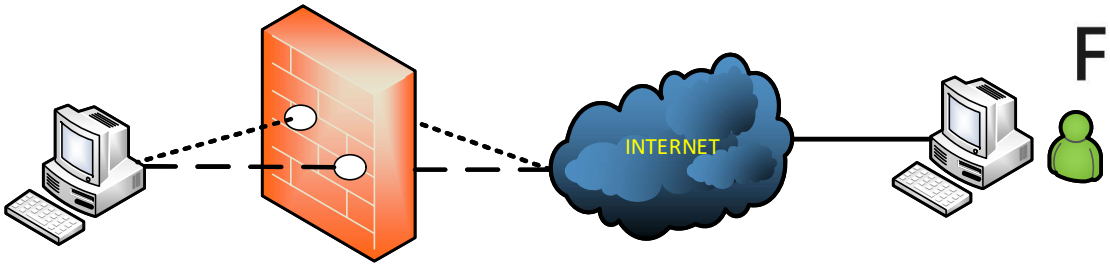
Agenda

- White Hat Hacking
- Legal Aspects
- Testing Frameworks
- Bug Bounty Programs

DIHSÜD

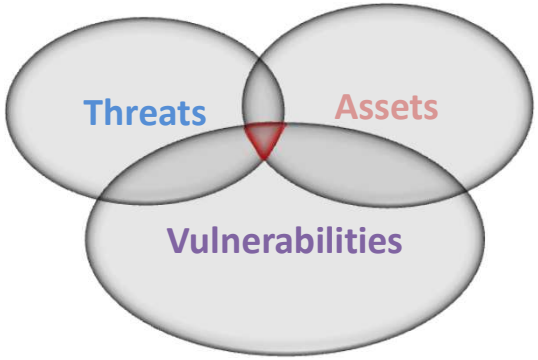
FH | JOANNEUM
University of Applied Sciences

White Hat Hacking
Security Testing

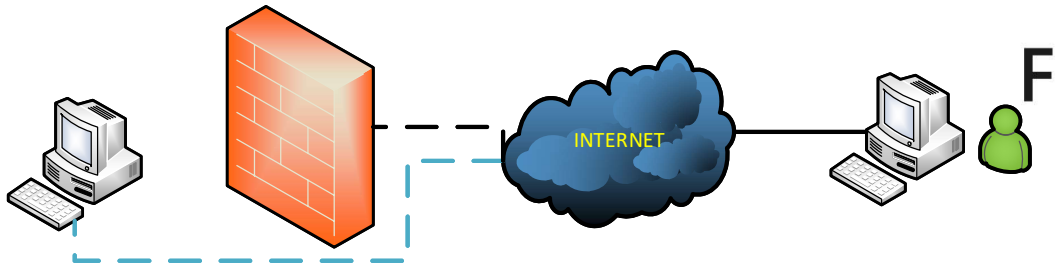


Vulnerability Assessment

- Limited testing time - pay per time
- Find as much vulnerabilities as possible
- Automated vulnerability scanning
- Breadth/Wide testing
- Different attack vectors
- Analyze individual systems



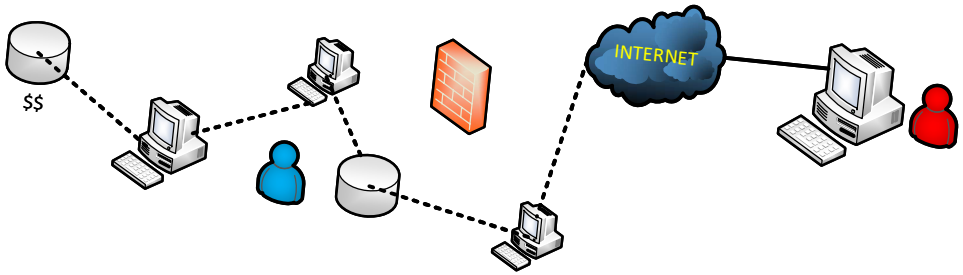
- Result:
  - Overview of the current security situation of the company



Penetration Test

- Definition of a worst-case scenario
- Limited testing time - pay per time
- Automated testing
- Manual testing
- Scan in depth
- Search for new, unknown vulnerabilities

- Result:
  - Verification of existing security measures



Red Team Assessment

- Goal: e.g. access to confidential data
- Free choice of tools, methods, time
- Search for different way to the target
- Realistic scenario
- Training of the Blue Team in their own environment
- Activities under the radar
- Result:
  - Verification of the entire security concept
- Purple Teams – Red & Blue teams work together

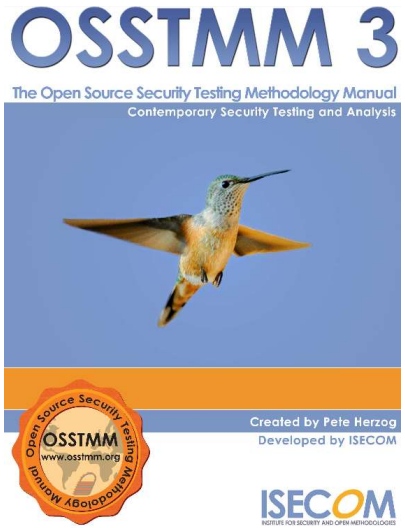
Testing Methodologies

Automated vs. Manual testing

- Manual
  - ping
  - traceroute
  - nmap
  - netdiscover
  - Wireshark
  - Web Browser
  - Web Proxies
  - Toolsets: impacket, …
- Automated
  - Nessus
  - OpenVas
  - Nikto
  - …

Testing Frameworks

- OSSTMM – Open Source Security Tesing Methodology Manual
- https://www.isecom.org/OSSTMM.3.pdf
- Version – 3 Free download



Legal aspects

Legal aspects

- It is forbidden to test computer systems not owned by you!
- You need a contract with the customer
- You need a PTA – Permission to Attack
  - IP – Range to test – Everything else is OUT OF SCOPE!
  - Testing period
  - Source addresses from which the test is carried out

Free Hacking
Bug Bounty Programs

Free (legal) „Hacking“

- Bug Bounty Programs
  - You get paid per bug not testing time!

- Bug Bounty Platforms
  - HackerOne
  - BugCrowd
  - BountyFactory
  - YesWeHack
  - Intigrity
  - …
  - Big companies host their own programs
  - Public vs. Private programs
  - Payed vs. VDP programs
  - OnDemand programs

HackerOne

https://hackerone.com/directory/programs

Inbox | Hacktivity | Directory | Opportunities | Hacker Dashboard | Job Board | Leaderboards

Programs | Pentesters

Directory

Find new hackable targets or contact information to report vulnerabilities you've already found.

Search Directory

Program features

- [ ] IBB
- [ ] Offers bounties
- [ ] High response efficiency
- [ ] Managed by HackerOne
- [ ] Offers retesting
- [x] Active program
- [ ] Bounty splitting

Asset type

- (•) Any
- ( ) CIDR
- ( ) Domain
- ( ) iOS: App Store
- ( ) iOS: Testflight
- ( ) iOS: .ipa
- ( ) Android: Play Store

Program	Launch date	Reports resolved	Bounties minimum	Bounties average
Amazon Vulnerability Research Program - Devices (Managed, Retesting)	09 / 2022	0	$50	-
Blend Labs (Managed, Retesting)	09 / 2022	3	$50	$750
Linktree (Managed, Retesting)	09 / 2022	115	$50	-
MongoDB (Managed, Retesting)	09 / 2022	14	$50	$500
ALSCO (Retesting)	09 / 2022	2	$50	$100-$200
Fossil (Managed)	08 / 2022	4	-	-

BugCrowd

https://bugcrowd.com/programs?sort[]=promoted-desc&accepted_invite[]=false

Dashboard **Programs** Discovery Submissions Payments Leaderboards CrowdStream Profile

All 598

accepted-invite:false

312 results matching search · You can find

Filter by whether you have accepted invitations

accepted-invite:false Programs for which you do not have an accepted invitation

Constant Contact, Inc.
A leader in email marketing for small business
Partial safe harbor
Submit report

Gearset: Managed Bug Bounty
Industry-leading DevOps solutions for every Salesforce team
$200 - $6,000 per vulnerability
Safe harbor
Submit report

Lucid Motors Vulnerability Disclosure Program
At Lucid we aim to create sustainable mobility without compro...
Safe harbor
Submit report

NameJet
Submit your finding to the program!
$150 - $2,500 per vulnerability
Safe harbor
Solo-Only
Submit report

Siteplus Vulnerability Disclosure Program
We're dedicated to providing the very best technology platfor...
Safe harbor
Solo-Only
Submit report

HostGator Brazil VDP
Submit your finding to the program!
Solo-Only
Submit report

Frontify
Cloud-based brand management platform.
$150 - $3,000 per vulnerability
Safe harbor
Solo-Only

USAA
We proudly serve millions of military members and their famil...
$100 - $6,000 per vulnerability
Partial safe harbor

TNG Technology Consulting GmbH Marketplace Bug Bounty Program
Please submit your findings to our program!
$100 - $1,500 per vulnerability
Safe harbor

Octopus Deploy
Submit your finding to the program!
$200 - $6,000 per vulnerability
Safe harbor

Wyze Bug Bounty
Bug Bounty
$50 - $1,000 per vulnerability

State Farm VDP
Large US Insurance Provider
Partial safe harbor
Solo-Only

Free „Hacking“

P4 $200 – $250

P3 $600 – $850

P2 $1500 – $1750

P1 $4100 – $4500

Points – $5,000
per vulnerability

Partial safe harbor

Managed by Bugcrowd

- Ranking - Example
  - Bugcrowd‘s Vulnerability Rating Taxonomy

Technical Severity▼	VRT Category	Specific Vulnerability Name	Variant / Affected Function
P1	Server Security Misconfiguration	Using Default Credentials	
P1	Server-Side Injection	File Inclusion	Local
P1	Server-Side Injection	Remote Code Execution (RCE)	
P1	Server-Side Injection	SQL Injection	
P1	Server-Side Injection	XML External Entity Injection (XXE)	
P1	Broken Authentication and Session Management	Authentication Bypass	

https://bugcrowd.com/vulnerability-rating-taxonomy

Free „Hacking“

- Ranking - Example
  - Bugcrowd‘s Vulnerability Rating Taxonomy

P2	Server Security Misconfiguration	Misconfigured DNS	High Impact Subdomain Takeover
P2	Server Security Misconfiguration	OAuth Misconfiguration	Account Takeover
P2	Sensitive Data Exposure	Weak Password Reset Implementation	Token Leakage via Host Header Poisoning
P2	Cross-Site Scripting (XSS)	Stored	Non-Privileged User to Anyone
P2	Broken Access Control (BAC)	Server-Side Request Forgery (SSRF)	Internal High Impact
P2	Cross-Site Request Forgery (CSRF)	Application-Wide	

Free „Hacking“

- Ranking - Example
  - Bugcrowd‘s Vulnerability Rating Taxonomy

P3	Server-Side Injection	HTTP Response Manipulation	Response Splitting (CRLF)
P3	Server-Side Injection	Content Spoofing	iframe Injection
P3	Broken Authentication and Session Management	Second Factor Authentication (2FA) Bypass	
P3	Broken Authentication and Session Management	Session Fixation	Remote Attack Vector
P3	Sensitive Data Exposure	Disclosure of Secrets	For Internal Asset
P3	Sensitive Data Exposure	EXIF Geolocation Data Not Stripped From Uploaded Images	Automatic User Enumeration
P3	Cross-Site Scripting (XSS)	Stored	Privileged User to Privilege Elevation

Free „Hacking“

- Ranking - Example
  - Bugcrowd‘s Vulnerability Rating Taxonomy

P4	Server Security Misconfiguration	No Rate Limiting on Form	Registration
P4	Server Security Misconfiguration	No Rate Limiting on Form	Login
P4	Server Security Misconfiguration	No Rate Limiting on Form	Email-Triggering
P4	Server Security Misconfiguration	No Rate Limiting on Form	SMS-Triggering
P4	Server Security Misconfiguration	Missing Secure or HTTPOnly Cookie Flag	Session Token
P4	Server Security Misconfiguration	Clickjacking	Sensitive Click-Based Action

Free „Hacking“

- Ranking - Example
  - Bugcrowd‘s Vulnerability Rating Taxonomy

P5	Server Security Misconfiguration	Lack of Password Confirmation	Change Email Address
P5	Server Security Misconfiguration	Lack of Password Confirmation	Change Password
P5	Server Security Misconfiguration	Lack of Password Confirmation	Manage 2FA
P5	Server Security Misconfiguration	Unsafe File Upload	No Antivirus
P5	Server Security Misconfiguration	Unsafe File Upload	No Size Limit
P5	Server Security Misconfiguration	Unsafe File Upload	File Extension Filter Bypass
P5	Server Security Misconfiguration	Cookie Scoped to Parent Domain	

Scope vs. out of scope

- WAF bypass
- Open redirects / Lack of security speedbump when leaving the site
- Internal IP address disclosure
- Accessible Non-sensitive files and directories (e.g. README.TXT, CHANGES.TXT, robots.txt, .gitignore, etc.)
- Social engineering / phishing attacks
- Self XSS
- Text injection
- Email spoofing (including SPF, DKIM, DMARC, From: spoofing, and visually similar, and related issues)
- Descriptive error messages (e.g., stack traces, application or server errors, path disclosure)
- Fingerprinting/banner disclosure on common/public services
- Clickjacking and issues only exploitable through clickjacking
- CSRF issues that don't impact the integrity of an account (e.g., log in or out, contact forms and other publicly accessible forms)
- Lack of Secure and HTTPOnly cookie flags (critical systems may still be in scope)
- Lack of rate limiting
- Login or Forgot Password page brute force, account lockout not enforced, or insufficient password strength requirements
- HTTPS mixed content scripts
- Username / email enumeration by brute forcing / error messages (e.g., login /signup / forgotten password)
- Exceptional cases may still be in scope (e.g., ability to enumerate email addresses via incrementing a numeric parameter)
- Missing HTTP security headers
- TLS/SSL Issues, including BEAST BREACH, insecure renegotiation, bad cipher suite, expired certificates, etc.
- Denial of Service attacks
- Out-of-date software
- Use of a known-vulnerable component (exceptional cases, such as where you are able to provide proof of exploitation, may still be in scope)
- Physical attacks against Facilities / Property
- Relay or RollJam attacks pertaining to the keyfob, NFC card, and/or phone-as-key

Safe Harbor

- **When conducting vulnerability research according to this policy, we consider this research to be:**
- Authorized in accordance with the Computer Fraud and Abuse Act (CFAA) (and/or similar state laws), and we will not initiate or support legal action against you for accidental, good faith violations of this policy;
- Exempt from the Digital Millennium Copyright Act (DMCA), and we will not bring a claim against you for circumvention of technology controls;
- Exempt from restrictions in our Terms & Conditions that would interfere with conducting security research, and we waive those restrictions on a limited basis for work done under this policy; and
- Lawful, helpful to the overall security of the Internet, and conducted in good faith.
- You are expected, as always, to comply with all applicable laws.
- *If at any time you have concerns or are uncertain whether your security research is consistent with this policy, please inquire via support@bugcrowd.com before going any further.*

‘I’m not a fan of critical bugs’ – Santiago Lopez on his route to becoming the world’s first bug bounty millionaire

Adam Bannister 25 September 2020 at 15:35 UTC
Updated: 28 September 2020 at 12:49 UTC

Bug Bounty | Hacking Techniques | Interviews

The Argentinian hacker reveals his methods behind the money-making

HackerOne Leaderboards

All leaderboards are based on the selected time period.

Highest Reputation

Ranking is calculated based on reputation earned.

		Reputation	Signal	Impact
▲ 1.	d0xing	33672	6.98	17.96
▼ 2.	todayisnew	27034	6.72	15.58
– 3.	m0chan	15073	6.84	15.94
▲ 4.	nagli	13345	6.80	17.73
▲ 5.	f6x	8012	7.00	22.70

Thank you!