Module 22
Bug Hunting and Pentesting

Ansh Bhawnani

Introduction

Module 22

1. Security Assessments

Module 22

Introduction

- **Security Assessment** (IT Security Assessment) is an explicit study to locate IT security vulnerabilities and risks.
- The organization grants access to its facilities, provides network access, outlines detailed information about the network, etc.
- Goal is to study security and identify improvements to secure the systems. An assessment for security is potentially the most useful of all security tests.
- A properly completed security assessment should provide documentation outlining any security gaps between a project design and approved corporate security policies.

Introduction

- The following *methodology* outline is put forward as the effective means in conducting security assessment.
  - *Requirement Study* and *Situation Analysis*
  - *Security policy creation* and *update*
  - *Document Review*
  - *Risk Analysis*
  - *Vulnerability Scan*
  - *Data Analysis*
  - *Report & Briefing*

2. Vulnerability Assessments

Module 22

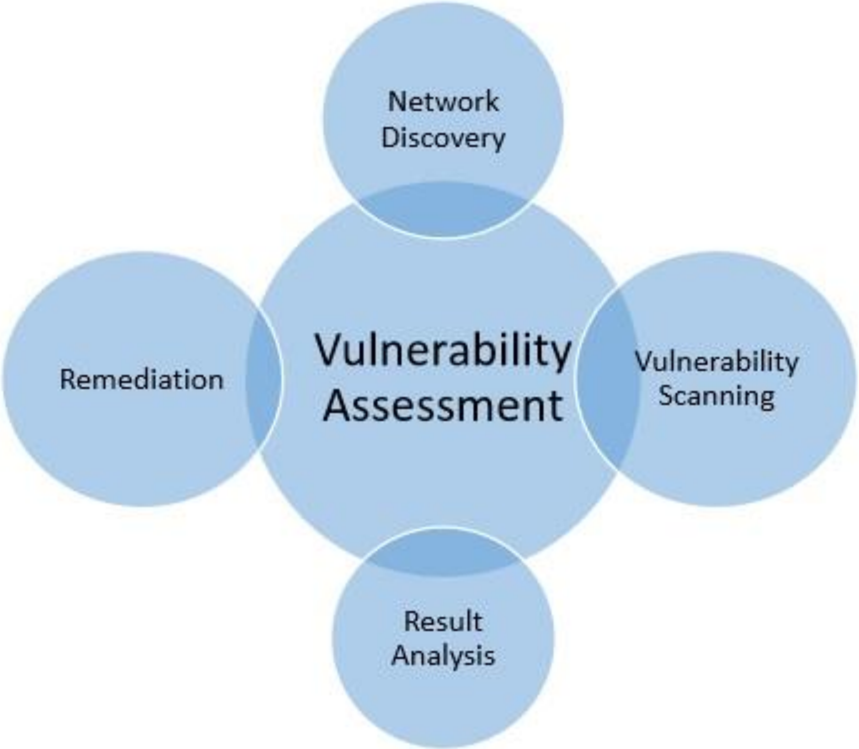
Introduction

- Vulnerability Assessment is also known as ***Vulnerability Testing***, is an assessment process that is intended to identify threats and the risks they pose typically involves the use of automated testing tools, whose results are listed in a vulnerability assessment report.
- Organizations of any size, or even individuals who face an increased risk of cyberattacks, can benefit from some form of vulnerability assessment.
- A vulnerability assessment provides direction on how to assess the risks associated with those weaknesses and evolving threats.
- Vulnerability Assessment with Penetration Testing is often termed as ***VAPT***.

Introduction

- **Types** of Vulnerability Assessments:
  - *Network-based* scans
  - *Host-based* scans
  - *Wireless network* scans
  - *Application* scans
  - *Database* scans

Introduction



3. Penetration Testing

Module 22

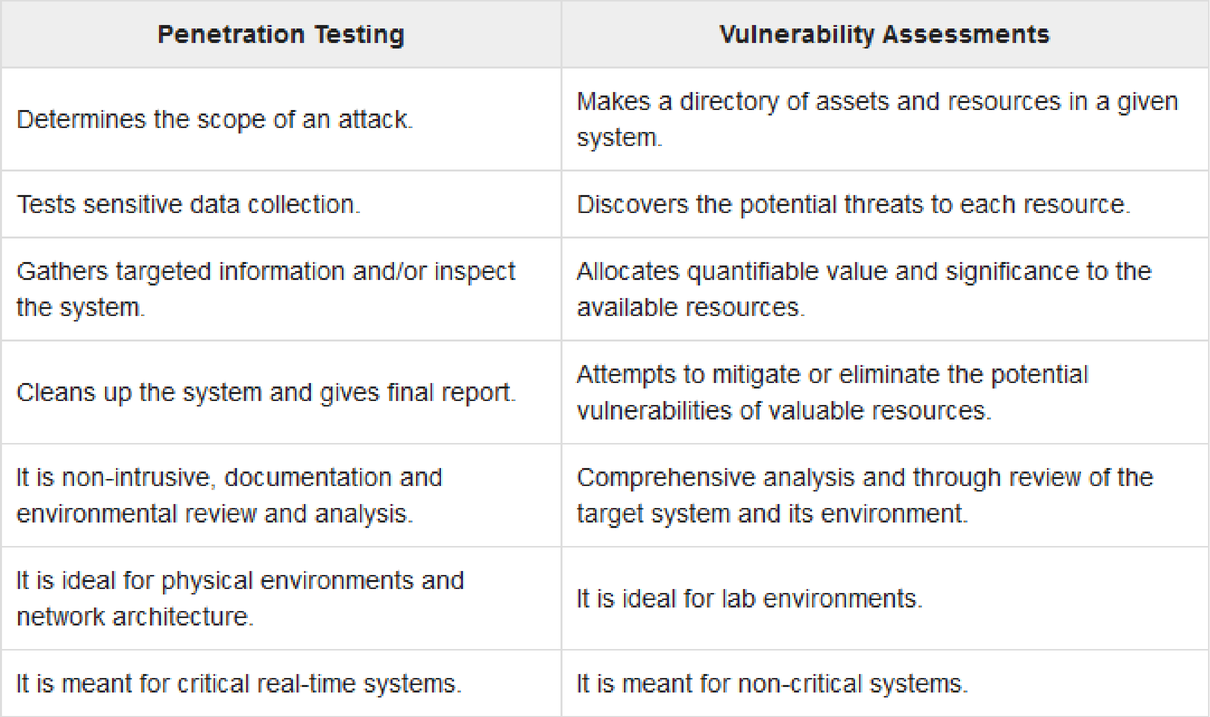
Introduction

- Penetration testing replicates the actions of an external or/and internal cyber attacker/s that is intended to break the information security and hack the valuable data or disrupt the normal functioning of the organization.
- Security issues that the penetration test uncovers should be reported to the system owner. Penetration test reports may also assess potential impacts to the organization and suggest countermeasures to reduce risk.
- A penetration test target may be a ***white box*** (which provides background and system information) or ***black box*** (which provides only basic or no information except the company name). A ***gray box*** penetration test is a combination of the two.

4. Penetration Testing vs Vulnerability Assessment

Module 22

Introduction



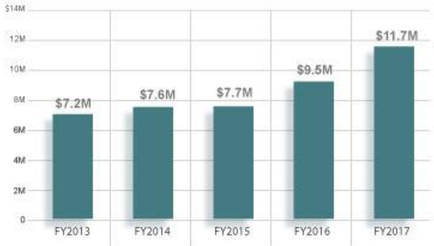
Penetration Testing	Vulnerability Assessments
Determines the scope of an attack.	Makes a directory of assets and resources in a given system.
Tests sensitive data collection.	Discovers the potential threats to each resource.
Gathers targeted information and/or inspect the system.	Allocates quantifiable value and significance to the available resources.
Cleans up the system and gives final report.	Attempts to mitigate or eliminate the potential vulnerabilities of valuable resources.
It is non-intrusive, documentation and environmental review and analysis.	Comprehensive analysis and through review of the target system and its environment.
It is ideal for physical environments and network architecture.	It is ideal for lab environments.
It is meant for critical real-time systems.	It is meant for non-critical systems.

5. Why Penetration Testing?

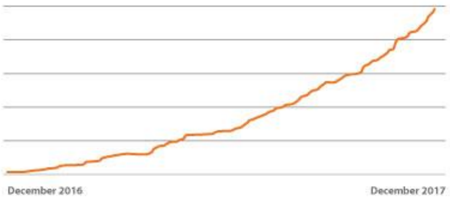
Module 22

Introduction

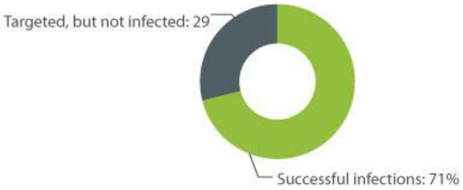
Global Cybercrime Costs 2013 - 2017



4.3x New Ransomware Variants in 2017 than 2016



Ransomware Success Rates



85%
of companies have fallen victim to phishing attacks

9 of 10
Phishing Mails were Ransomware Attack

Every 40 Sec
There is a Ransomware Attack

23 Days
Average time required to resolve one Ransomware Attack

Source: Indeed Blog and IT Jobs Watch

Introduction

- They can give security personnel real experience in dealing with an intrusion.
- It can uncover aspects of security policy that are lacking.
- They provide feedback on the most at risk routes into your company or application.
- Penetration testing reports can be used to help train developers to make fewer mistakes.
- Every penetration testing report helps an organization to keep track of the exploits performed and the information accumulated.
- The penetration tester will also be able to advise you on what risks must be addressed first based on the amount of risk exposure it involves.

6. When to Perform Penetration Testing?

Module 22

Introduction

- Security system discovers new threats by attackers.
- You add a new network infrastructure.
- You update your system or install new software.
- You relocate your office.
- You set up a new end-user program/policy.

7. Types of Pen Testing

Module 22

Introduction

Black Box Penetration Testing

- In black box penetration testing, tester has no idea about the systems that he is going to test.
- *Advantages:*
  - No need to be expert, does not demand specific language knowledge
  - Tester verifies contradictions in the actual system and the specifications
  - Test conducted with the perspective of a user, not the designer

Introduction

- Black Box Penetration Testing
  - **Disadvantages:**
    - Particularly, these kinds of test cases are difficult to design.
    - Possibly, it is not worth, incase designer has already conducted a test case.
    - It does not conduct everything.

Introduction

White Box Penetration Testing

- This is a comprehensive testing, as tester has been provided with whole range of information about the systems and/or network such as Schema, Source code, OS details, IP address, etc
- *Advantages:*
  - All independent paths of a module can be exercised.
  - All logical decisions can be verified along with their true and false value.
  - It discovers the typographical errors and does syntax checking.
  - It finds the design errors due to difference between logical flow of the program and the actual execution.

Introduction

- White Box Penetration Testing
  - **Disadvantages:**
    - Often cannot assess all the test cases.
    - Takes a lot of time.
    - Test is from the viewpoint of a developer, not user, so often limited scope.

Introduction

Gray Box Penetration Testing

- In this type of testing, a tester usually provides partial or limited information about the internal details of the program of a system.
- *Advantages:*
  - As the tester does not require the access of source code, it is non-intrusive and unbiased
  - As there is clear difference between a developer and a tester, so there is least risk of personal conflict
  - You don’t need to provide the internal information about the program functions and other operations

8. Requirements of a PenTester

Module 22

Introduction

Certification

- Certified Ethical Hacker (***CEH***).
- Offensive Security Certified Professional (***OSCP***).
- ***CREST*** Penetration Testing Certifications.
- Communication Electronic Security Group (***CESG***) IT Health Check Service certification.
- Global Information Assurance Certification (***GIAC***) Certifications for example, GIAC Certified Penetration Tester (***GPEN***), GIAC Web Application Penetration Tester (***GWAPT***), Advance Penetration Tester (***GXPN***), and GIAC Exploit Researcher.

Introduction

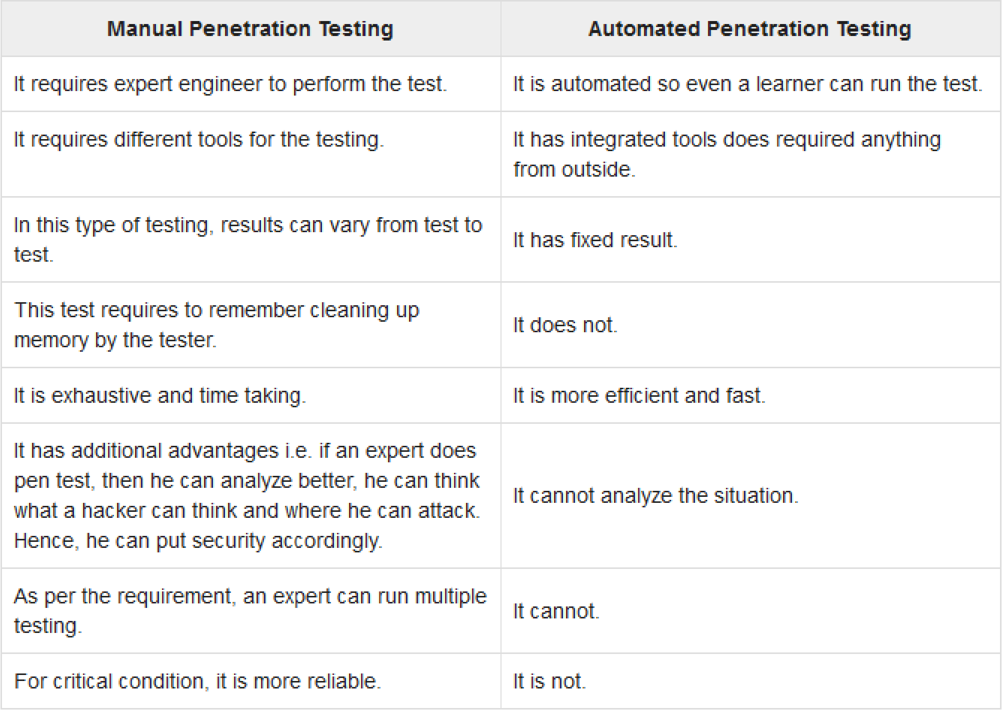
Past Experience

- How many years of experience does the penetration tester has?
- Is he an independent penetration tester or working for an organization?
- With how many companies he worked as penetration tester?
- Has he performed penetration testing for any organization, which has similar size and scope as yours?
- What type of experience does the penetration tester has? For example, conducting network-layer penetration testing, application based, etc
- You may also ask for the reference from other customers for whom he worked.

9. Manual vs Automated Pentesting

Module 22

Introduction



Manual Penetration Testing	Automated Penetration Testing
It requires expert engineer to perform the test.	It is automated so even a learner can run the test.
It requires different tools for the testing.	It has integrated tools does required anything from outside.
In this type of testing, results can vary from test to test.	It has fixed result.
This test requires to remember cleaning up memory by the tester.	It does not.
It is exhaustive and time taking.	It is more efficient and fast.
It has additional advantages i.e. if an expert does pen test, then he can analyze better, he can think what a hacker can think and where he can attack. Hence, he can put security accordingly.	It cannot analyze the situation.
As per the requirement, an expert can run multiple testing.	It cannot.
For critical condition, it is more reliable.	It is not.

10. Pen Testing tools

Module 22

Introduction

Network Based Scans

- *Nmap*
- *Hping*
- *SuperScan*
- *Xprobe*
- *Nessus*
- *Responder*
- *Metasploit*

Introduction

Wireless Network Scans

- *Wireshark*
- *Aircrack-ng*
- *Airsnort*
- *Kismet*
- *NetStumbler*
- *CowPatty*
- *Cain and Abel*

Introduction

- Application Based Scans
  - *Nikto*
  - *Wpscan*
  - *Exploit-db*
  - *Hashcat*
  - *Burpsuite*
  - *OWASP ZAP*
  - *Acunetix*

Introduction

- **Databased Based Scans**
  - *Sqlmap*
  - *Sqlninja*
  - *Sqlite db viewer*

Penetration Testing Methodology

Module 22

1. Phases of Penetration Testing

Module 22

Phases of Penetration Testing

1. Pre Engagement

Meeting with the client to have a crystal understanding of all their needs and vision

2. Planning and Recon

Test plan generation and public information gathering through scanning

3. Threat Modelling and Vulnerability Identification

Model of all the security concerns and ranking vulnerability severity

4. Exploitation

Gaining access by breaching security of a system or finding a bug to exploit in the software.

5. Post Exploitation

Determining the value of the assets compromised and further attack propagation

Phases of Penetration Testing

6. Reporting

Detailing the vulnerabilities found, stating impact and remedies

7. Resolution and Re Testing

Resolving the issues and verify the fixes

2. Penetration Testing Report Writing

Module 22

Penetration Testing Methodology

- **Objectives** – It describes the overall purpose and benefits of pen testing.
- **Time** – It gives the accurate status of the system. It indicated the validity of the report in the current scope.
- **Target Audience** –Such as information security manager, information technology manager, chief information security officer, and technical team.
- **Report Classification** –. Classification needs to be done on the basis of target organization which has an information classification policy, e.g., server IP addresses, application information, vulnerability, threats, etc.
- **Report Distribution** – Number of copies and report distribution should be mentioned in the scope of work.

Penetration Testing Methodology

Information Collection

- Pen tester is required to mention all information collected in all the stages of testing. Additionally tools, scanning results, vulnerability assessments, details of his findings, etc.

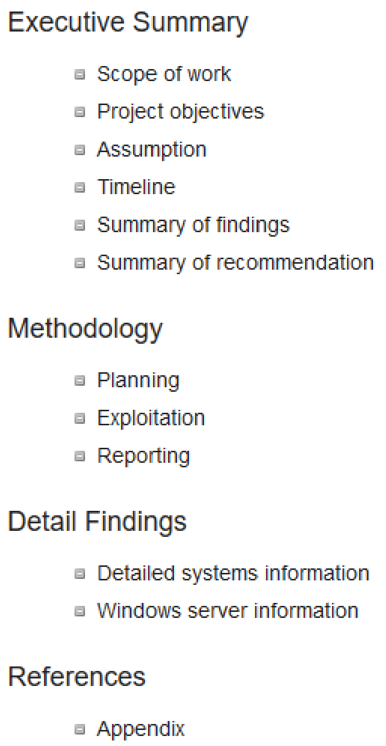
Writing the First Draft

- Primarily, he needs to write the first draft in the details – mentioning everything i.e. all activities, processes, and experiences.

Review and Finalization

- After drafting, it has to be reviewed first by the drafter himself and then by his seniors or colleagues who may have assisted him.

Penetration Testing Methodology



Executive Summary

- Scope of work
- Project objectives
- Assumption
- Timeline
- Summary of findings
- Summary of recommendation

Methodology

- Planning
- Exploitation
- Reporting

Detail Findings

- Detailed systems information
- Windows server information

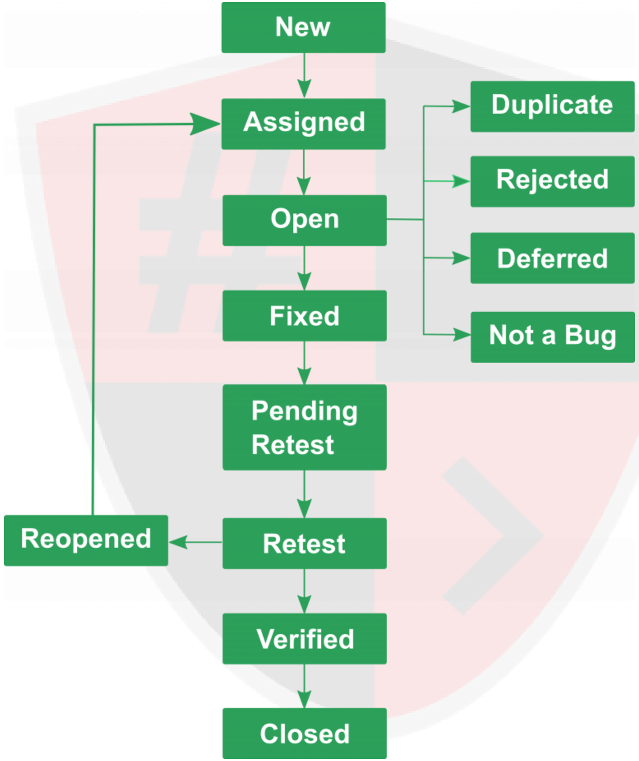
References

- Appendix

Bug Bounty Report Writing

Module 22

Bug Bounty Report Writing



1. Understanding Audience standards

Module 22

Bug Bounty Report Writing

- Plan your report according to the organizational standards.
- There will be lots of stakeholders who need to read what you write - other *QAers*, *Developers*, *Support*, *Product Management*, *Documentation*, *Management*, etc. It may become more important to use less jargon, and add more details.
- If offshore testers or developers must read your Issue Reports, you'll need to pay special attention not to use confusing jargon or colloquialisms in your writing.
- You may even be better off having two different descriptions of the bug - one for internal consumption, and one for customers.

2. Essential Components of a report

Module 22

Bug Bounty Report Writing

Title

- It has to be simple but clear, explain what about is the report in one single line. It should contain the type of the vulnerability, the potential impact and what asset is concerned.
- **Good:**
  - Open redirect + Stored XSS in profile lead to account takeover on www.example.com
  - [192.168.1.1] Public Jenkins instance leads to RCE

Bug Bounty Report Writing

- Title
  - So so:
    - XSS on www.example.com
    - PHP errors reveal webapp full path
  - Forget it:
    - XSS
    - Local file inclusion
    - Critical bug on www.example.com

Bug Bounty Report Writing

Rating

- Take time to rate the issue, in an obvious way. Too low, there is a chance that the sec team pass over it, but you could be happy if finally the bounty is higher than your expectations.
- Too high, the sec team could think that you overrated in order to increase the bounty, they will notice, lower the rating, lower the bounty and you will be disappointed.
- Try to provide a suitable CVSS score. Even if it's not perfect and context dependent, it gives a good idea of the criticality of the issue in a technical point of view. Note that some platforms award bonus points for that.

Bug Bounty Report Writing

- **Introduction:** A reminder of the title a little bit more verbose, but no technical details at all. You can also write a quick explanation of the class of the vulnerability.
- **Description:** In a nutshell, the full explanation of the vulnerability. Name the variables, their values, provide endpoints and all conditions required to trigger the issue: what, when, where, who etc… The whole everything.
- **Steps to reproduce:** The goal here is to help the team to reproduce the bug in an easy way. Give them the whole process step by step using an ordered list so you could reference any step at any moment.
- Providing the response is also a good thing to show the team the difference between a legit result and an unexpected behavior.

Bug Bounty Report Writing

1. Connect to your account: https://www.example.com/login
2. Click on the “profile” tab
3. Enter value payload in the input input
4. repeat step 2

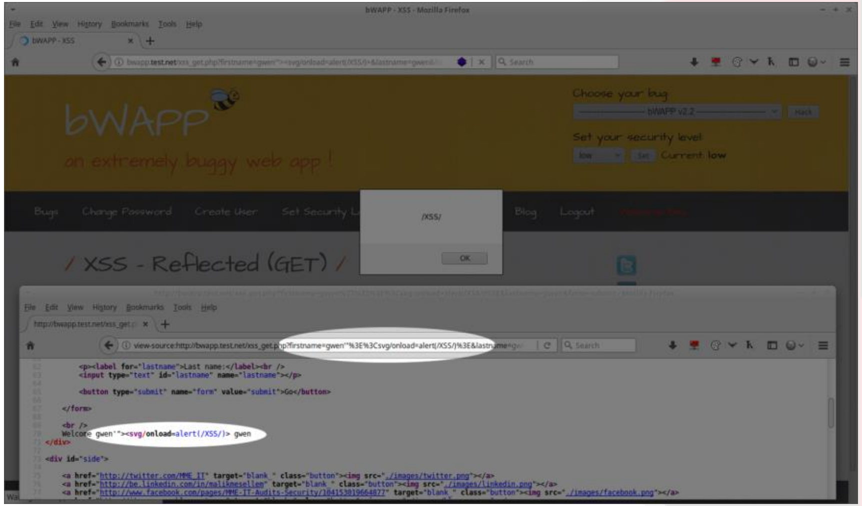
…

- If you use a local proxy like Burp Suite, you can provide the request in a http block code. It’s very easy to reproduce the issue that way, you simply need to copy/paste it back to the software, update the cookie or any auth token and that’s it, simple and efficient.

Bug Bounty Report Writing

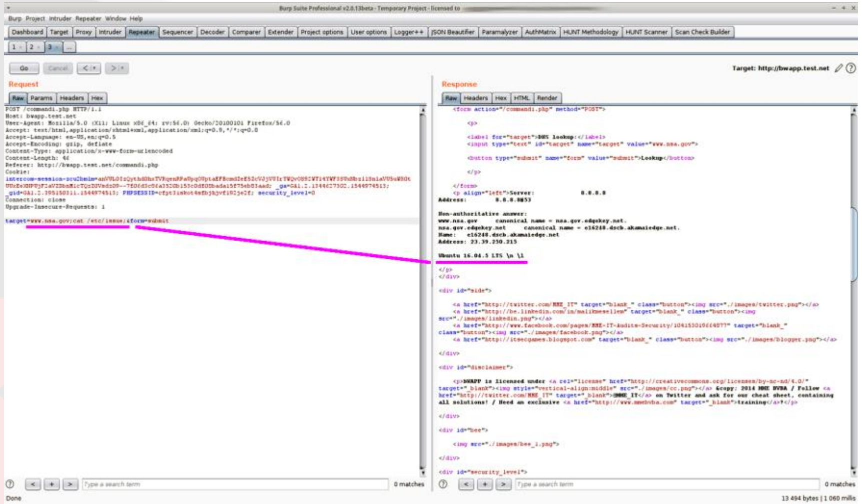
- **PoC (Proof of Concept):** Provide everything that can prove the bug. Also, keep in mind that the report can be publicly disclosed in the future, so take care of hiding personal information you want to keep private.
  - **Screenshots and Images** that you can quickly modify with an image editor in order to highlight payloads and data extracted. No need to be a great designer here.
  - **Videos** are very better that replays the whole drama that leads you to this great report.

Bug Bounty Report Writing


bWAPP - XSS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
bWAPP
an extremely buggy web app !
Choose your bug
Set your security level
Current: low
Bugs Change Password Create User Set Security Level Blog Logout
/XSS/
OK
/ XSS - Reflected (GET) /

```
view-source:http://bwapp.test.net/xss_get.php?firstname=gwen'"%3E%3Csvg/onload=alert(/XSS/)%3E&lastname=gw
```

```
        <p><label for="lastname">Last name:</label><br />
        <input type="text" id="lastname" name="lastname"></p>

        <button type="submit" name="form" value="submit">Go</button>

    </form>

    <br />
    Welcome gwen'"><svg/onload=alert(/XSS/)> gwen
</div>

<div id="side">

    <a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
    <a href="http://be.linkedin.com/in/malikmesellem" target="blank_" class="button"><img src="./images/linkedin.png"></a>
    <a href="http://www.facebook.com/pages/MME-IT-Audits-Security/104153019664877" target="blank_" class="button"><img src="./images/facebook.png"></a>
```


Burp Suite Professional v2.0.13beta - Temporary Project - licensed to
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Logger++ JSON Beautifier Paramalyzer AuthMatrix HUNT Methodology HUNT Scanner Scan Check Builder
Go Cancel
Target: http://bwapp.test.net
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
0 matches
Done
13 494 bytes | 1 060 millis

```
POST /commandi.php HTTP/1.1
Host: bwapp.test.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 46
Referer: http://bwapp.test.net/commandi.php
Cookie:
intercom-session-[illegible]; _ga=GA1.2.[illegible];
_gid=GA1.2.[illegible]; PHPSESSID=[illegible]; security_level=0
Connection: close
Upgrade-Insecure-Requests: 1

target=www.nsa.gov;cat /etc/issue;&form=submit
```

```
    <form action="/commandi.php" method="POST">

        <p>

        <label for="target">DNS lookup:</label>
        <input type="text" id="target" name="target" value="www.nsa.gov">

        <button type="submit" name="form" value="submit">Lookup</button>

        </p>

    </form>
    <p align="left">Server:             8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
www.nsa.gov     canonical name = nsa.gov.edgekey.net.
nsa.gov.edgekey.net     canonical name = e16248.dscb.akamaiedge.net.
Name:   e16248.dscb.akamaiedge.net
Address: 23.39.250.215

Ubuntu 16.04.5 LTS \n \l

</p>
</div>

<div id="side">

    <a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
    <a href="http://be.linkedin.com/in/malikmesellem" target="blank_" class="button"><img
src="./images/linkedin.png"></a>
    <a href="http://www.facebook.com/pages/MME-IT-Audits-Security/104153019664877" target="blank_"
class="button"><img src="./images/facebook.png"></a>
    <a href="http://itsecgames.blogspot.com" target="blank_" class="button"><img src="./images/blogger.png"></a>
```

Bug Bounty Report Writing

Impact

- It's the job of the hacker to prove the criticality of the vulnerabilities he finds.
- Do not boast about a high severity, just be practical and think of the real impact.
- State in points for multiple issues in order of severity.
- Try to create a possible scenario showing the potential risks of the issue. But take care to not fall to the "Hollywood syndrome".

Bug Bounty Report Writing

Mitigation

- Trying to stay obvious and honest, if you think that some technical details make the issue very hard to exploit then it’s important to let the team know about it.
- For instance a RCE that can only be triggered in January, between 12th and 2am at full moon night ☺

Bug Bounty Report Writing

Remediation

- Do you have any idea on how to solve the problem ?
- This is greatly appreciated by companies, they will be happy to read your tips/recommendations. Remember that bug bounty is also about learning (for both parts).

Bug Bounty Report Writing

Additional notes

- Sometimes you have to provide small details that can be helpful to the team to better understand the issue, why it works most of the time but fails in a specific case.
- The faster they reproduce the issue, the faster your report will be triaged, the faster you will be payed :)

Bug Bounty Report Writing

References

- This is where I put links to external resources:
  - *OWASP article*
  - *Blog articles (GitHub, Medium)*
  - *CVE*
  - *Disclosed reports*
  - ***Real study case*** or whatsoever that can support your reports. The goal is to help the team to understand and fix the issue but also show her the criticality.

3. Tips for Writing a Good Report

Module 22

Bug Bounty Report Writing

Thoroughness

- Make sure that you cover every single step that someone would need to follow to reproduce your bug.
- *Will they need to be logged in to see it?*
- *Will it only work in a specific browser or is blocked by a content-secure policy?*
- *Is it clear which elements on a page you are referring to?*
- *If you have doubts about any of these, try walking through the steps yourself, and see if there are any steps that could be ambiguous*

Bug Bounty Report Writing

Simplicity

- It is important to find a balance between thoroughness and complexity. While it may sometimes require a full page of steps to describe a bug, this is often not necessary.
- For example, reporting a reflected XSS (cross site scripting) may be as simple as providing a link and saying which browsers it will execute in. There’s no reason to include a stack trace or history of the web if your bug can be demonstrated by clicking a link!

Bug Bounty Report Writing

Neutrality

- You’re trying to properly convey the impact of the bug to them. But with monetary rewards involved, it can be difficult to provide an unbiased assessment of your bug’s actual impact.
- *Just be honest*! Presenting your bug to be worse than it actually is can lose trust with a company, and could even result in a lower bounty.

4. Bug Bounty Terminologies

Module 22

Bug Bounty Report Writing

- **Security Team:** A team of individuals who are responsible for addressing security issues found in a product or service.
- **Finder:** Also known as hackers. Anyone who has investigated a potential security issue in some form of technology.
- **Report:** A Finder's description of a potential security vulnerability in a particular product or service.
- **Vulnerability:** A software bug that would allow an attacker to perform an action in violation of an expressed security policy.
- **Programs:** Security Teams may publish a Program and Program Policy designed to guide security research into a particular service or product. Private program participation is entirely optional and non-disclosable by default.

Ethics and Standards

Module 22

1. Responsible Disclosure

Module 22

Ethics and Standards

- Responsible Disclosure is a vulnerability disclosure model in which a vulnerability or an issue is disclosed only after a period of time that allows for the vulnerability or issue to be patched or mended. This period distinguishes the model from full disclosure.
- A *VDP* is the digital equivalent of "*if you see something, say something*." It's intended to give anyone — ethical hackers (aka "researchers" or "finders"), anyone who stumbles across something amiss — clear guidelines for reporting potentially unknown or harmful security vulnerabilities to the proper person or team responsible.
- Guidelines for Responsible Disclosure policies are listed in an *Open Source Repo*:

  https://github.com/disclose/disclose

Ethics and Standards

- Hackers and computer security scientists have the opinion that it is their social responsibility to make the public aware of vulnerabilities.
- To avoid this, the involved parties join forces and agree on a period of time for repairing the vulnerability and preventing any future damage, this period may vary between a few days and several months. This time may depend on:
  - *Impact* of the vulnerability
  - *Security policy awareness* in the organization
  - *Complexity* of the issue
  - *Resources available* to fix the issue
  - *Coordination* and *communication* between security team and developers

Ethics and Standards

CRITICAL ELEMENTS OF A VULNERABILITY DISCLOSURE POLICY

- *Promise*: You state a clear, good faith commitment to customers and other stakeholders potentially impacted by security vulnerabilities.
- *Scope*: You indicate what properties, products, and vulnerability types are covered.
- "*Safe Harbor*": Assures that the finder reporting in good faith will not be unduly penalized.
- *Process*: The process finders use to report vulnerabilities.
- *Preferences*: A living document that sets expectations for preferences and priorities regarding how reports will be evaluated.

2. Organizational standards

Module 22

Ethics and Standards

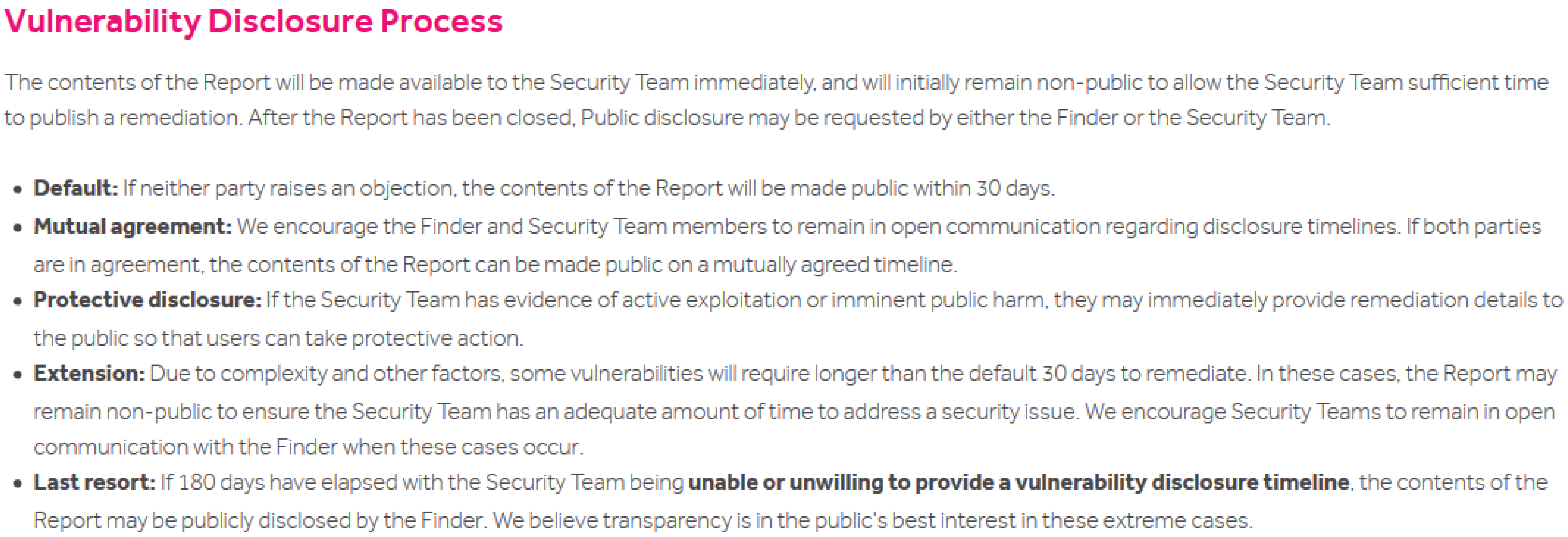
Submission Process

Security Teams will publish a program policy designed to guide security research into a particular service or product. You should always carefully review this program policy prior to submission as they will supersede these guidelines in the event of a conflict.

If you believe you have found a vulnerability, please submit a Report to the appropriate program on the HackerOne platform. The Report should include a detailed description of your discovery with clear, concise reproducible steps or a working proof-of-concept. If you don't explain the vulnerability in detail, there may be significant delays in the disclosure process, which is undesirable for everyone.

The Report will be updated with significant events, including when the vulnerability has been validated, when more information is needed from you, or when you have qualified for a bounty.

Ethics and Standards

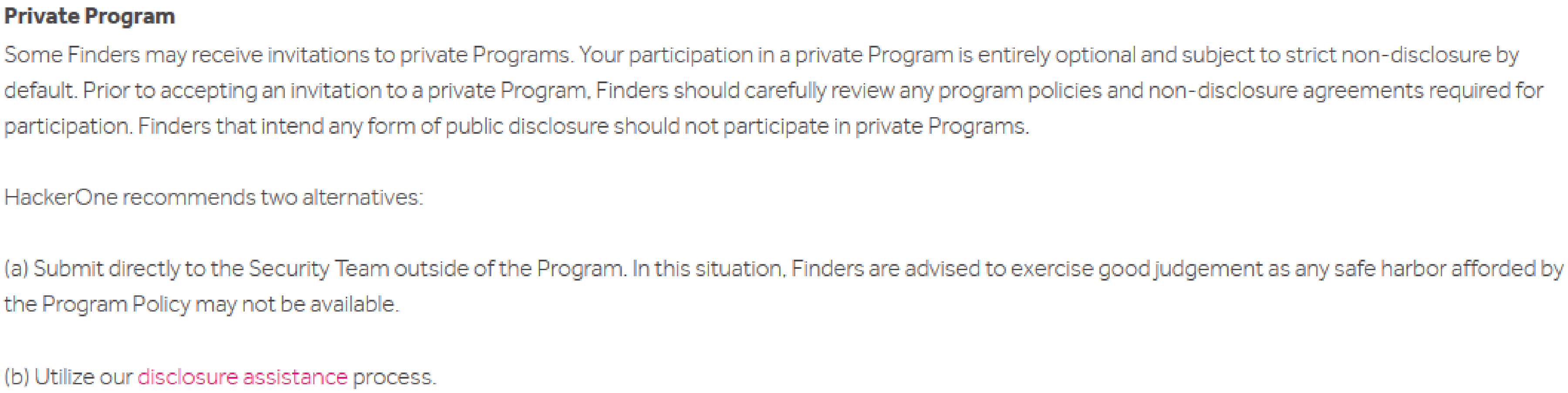


Vulnerability Disclosure Process

The contents of the Report will be made available to the Security Team immediately, and will initially remain non-public to allow the Security Team sufficient time to publish a remediation. After the Report has been closed, Public disclosure may be requested by either the Finder or the Security Team.

- **Default:** If neither party raises an objection, the contents of the Report will be made public within 30 days.
- **Mutual agreement:** We encourage the Finder and Security Team members to remain in open communication regarding disclosure timelines. If both parties are in agreement, the contents of the Report can be made public on a mutually agreed timeline.
- **Protective disclosure:** If the Security Team has evidence of active exploitation or imminent public harm, they may immediately provide remediation details to the public so that users can take protective action.
- **Extension:** Due to complexity and other factors, some vulnerabilities will require longer than the default 30 days to remediate. In these cases, the Report may remain non-public to ensure the Security Team has an adequate amount of time to address a security issue. We encourage Security Teams to remain in open communication with the Finder when these cases occur.
- **Last resort:** If 180 days have elapsed with the Security Team being **unable or unwilling to provide a vulnerability disclosure timeline**, the contents of the Report may be publicly disclosed by the Finder. We believe transparency is in the public's best interest in these extreme cases.

Ethics and Standards



Private Program

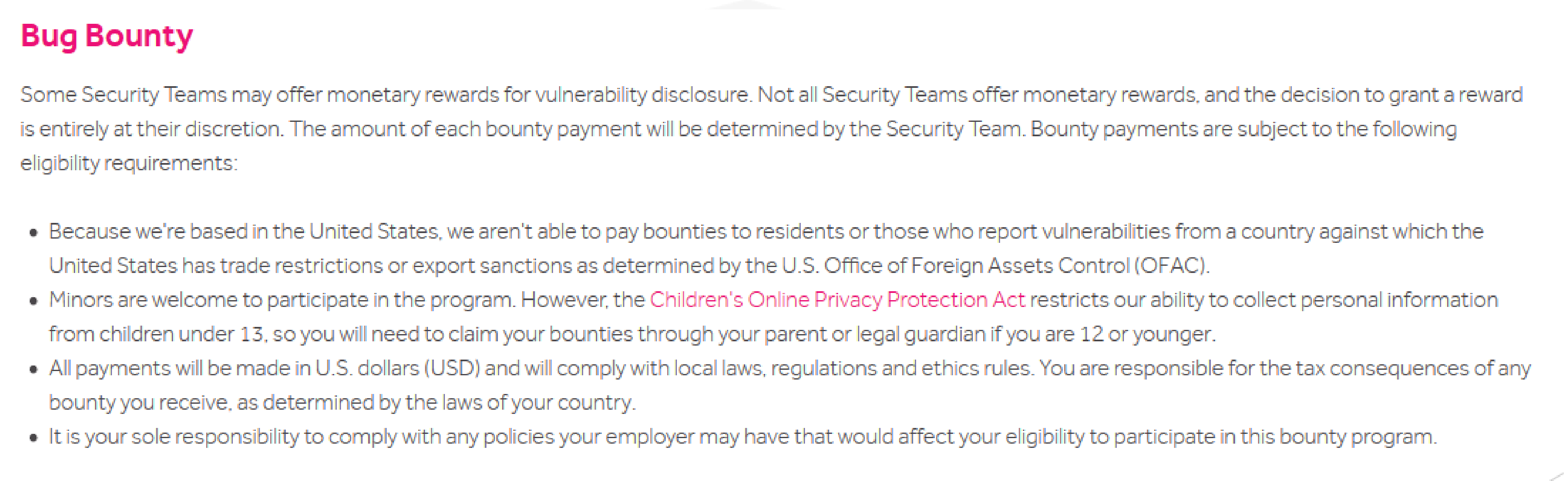
Some Finders may receive invitations to private Programs. Your participation in a private Program is entirely optional and subject to strict non-disclosure by default. Prior to accepting an invitation to a private Program, Finders should carefully review any program policies and non-disclosure agreements required for participation. Finders that intend any form of public disclosure should not participate in private Programs.

HackerOne recommends two alternatives:

(a) Submit directly to the Security Team outside of the Program. In this situation, Finders are advised to exercise good judgement as any safe harbor afforded by the Program Policy may not be available.

(b) Utilize our disclosure assistance process.

Ethics and Standards



Bug Bounty

Some Security Teams may offer monetary rewards for vulnerability disclosure. Not all Security Teams offer monetary rewards, and the decision to grant a reward is entirely at their discretion. The amount of each bounty payment will be determined by the Security Team. Bounty payments are subject to the following eligibility requirements:

- Because we're based in the United States, we aren't able to pay bounties to residents or those who report vulnerabilities from a country against which the United States has trade restrictions or export sanctions as determined by the U.S. Office of Foreign Assets Control (OFAC).
- Minors are welcome to participate in the program. However, the Children's Online Privacy Protection Act restricts our ability to collect personal information from children under 13, so you will need to claim your bounties through your parent or legal guardian if you are 12 or younger.
- All payments will be made in U.S. dollars (USD) and will comply with local laws, regulations and ethics rules. You are responsible for the tax consequences of any bounty you receive, as determined by the laws of your country.
- It is your sole responsibility to comply with any policies your employer may have that would affect your eligibility to participate in this bounty program.

3. Tips for Better Bug Hunting

Module 22

Ethics and Standards

Don’t Expect Anything!

- “Rewards don’t come who wait for them!” Don’t expect anything just close the report and start looking for other bug’s because that could end up making you sad.
- “No bug hunter got his first reward in a few clicks!”
- Sometimes its as easy as running a tool, sometimes you have to give your heart out.
- Bounty rewards are highly unpredictable!
- Make a mindset “I’m Going to Hunt Bug’s for Whole Week, Let’s just keep the target of 100$”. You’ll end up lot more than that!

Ethics and Standards

Less knowledge about vulnerabilities and testing methodologies

- This is also common scenario lot of new bounty hunter’s start looking for bug’s without basic knowledge of how things work.
- You will not understand how an application works until and unless you know how they build them.
- It is necessary first to know how applications are built. So make your mind to learn some programming!

Ethics and Standards

Have your own methodology

- Listen and understand others’ methodology and algorithms, but never try to copy them.
- If everyone has the same way, everything just boils down to first come first serve. *Duplicates* are the biggest nightmare for a hunter.
- Uniqueness is the only mantra to remain competitive.
- Develop your own methods and approach to dig, recon, diagnosis, and attack.

Ethics and Standards

Surround yourself with Bug Bounty community to keep yourself updated

- Create Twitter Handle and go to Hackerone Leaderboard :https://hackerone.com/leaderboard/all-time
- Go to their hunter profiles on HackerOne, Bugcrowd, etc and follow them on Twitter.
- Keep bookmarking.
- Keep reading public disclosed reports (HackerOne).
- Join *Bug Bounty World* on Slack and keep reading their blogs ,tools, general channel and their conversations of testing and share what you know.

Ethics and Standards

Automation

- “Automation is Power.”
- If you want to automate things, you need to learn “scripting”. It is highly recommended learn some programming language.
- Some of the best scripting languages are: *JS*, *PYTHON*, *RUBY*, ***BASH*****,** even knowing some ***curl*** tricks or basic ***bash*** commands scripting, you have power in your hands!
- Manual attacks are old school.

Ethics and Standards

Get bounty or get experience

- Bounties are temporary, knowledge is permanent.
- Nobody get's rewards every time, but they get one thing each time, *experience.*
- Don't loose hope, stay motivated, "failure is the best feature of a hard worker".
- There is never a loss. Its a win win situation.

Ethics and Standards

Find the “bug” or find a “Bugs Chain”

- If you find a BUG, always yourself: what’s the security impact on the application? ask
- You can think outside the box and start hunting with the concept of *“looking for the best impact”*. Find another issue which when combined, will increase the impact, and hence the reward.
- **“Stay at the valley or work hard to claim the mountain and see a big panorama.”**

Ethics and Standards

Relax and Enjoy life

- Have time for yourself. Rest, get outside, meet friends, family, party, exercise, keep your body and mind fit.
- A free and calm mind is way more productive and focused.
- Stop frustrating and close your laptop. Divert yourself. There is a lot of life beyond bugs.
- Health is bounty! (wealth)

HACKING

Is an art, practised through a creative mind.