# Intro to security 2

Malware

Vulnerabilities

Network attacks

Web attacks

Tools

# Cryptography

Encryption: a means to allow two parties, customarily called Alice and Bob, to establish confidential communication over an insecure channel that is subject to eavesdropping.



#### Last lecture: Encryption and Decryption

The message M is called the plaintext.

Alice will convert **plaintext M** to an encrypted form

• Alice uses an **encryption algorithm E** that outputs **a ciphertext C** for M.

As equations:

C = E(M)

M = D(C)

The encryption and decryption algorithms are chosen so that it is infeasible for someone other than Alice and Bob to determine plaintext M from ciphertext C.

ciphertext C can be transmitted over an insecure channel that can be eavesdropped by an adversary.

#### Classical cryptosystems (single-key or symmetric cryptosystems)

		A	В	С	D	Ε	F	G	Н	1	J	Κ	L	М
Substitution Ciphers	A	А	В	С	D	Е	F	G	н	L	J	κ	L	М
	В	В	С	D	Е	F	G	Н	L	J	Κ	L	М	Ν
A substitution cipher	С	С	D	Е	F	G	Н	I	J	Κ	L	Μ	Ν	0
changes characters in the	D	D	Е	F	G	Н	L	J	Κ	L	М	Ν	0	Ρ
nlaintext to produce the	E	Е	F	G	Н	L	J	Κ	L	М	Ν	0	Ρ	Q
	F	F	G	Н	1	J	Κ	Ľ	М	Ν	0	Ρ	Q	R
ciphertext.	G	G	Н	1	J	κ	L	М	Ν	0	Р	Q	R	S

• Transposition ciphers

EXAMPLE: The first line of a limerick is enciphered using the key "BENCH," as follows.

- Cesar cipher
- Vigenère cipher
  - A longer key, uses tableau

KeyBENCHBENCHBENCHBENCHBENCHBENCHPlaintextALIMERICKPACKSLAUGHSANATOMICALCiphertextBPVOLSMPMWBGXUSBYTJZBRNVVNMPCS

**One-Time Pad:** if the key as long as the text

# Public Key Cryptography

Two keys: encipherment and decipherment keys

Public (encipherment) key is public!

**Private** (decipherment) **key** is know only to owner!

#### RSA

c = m<sup>e</sup> mod n m = c<sup>d</sup> mod n

- φ(n)
  - the number of numbers less than n with no factors in common with n
- Choose e: e < n relatively prime to  $\varphi(n)$ .
- Find d: ed mod φ(n) = 1

The public key is (e, n)

the private key is d

n = pq, p and q primes

In addition to confidentiality, RSA can provide data and origin authentication.

# Symmetric cryptosystems

Alice and Bob share a secret key, which is used for both encryption and decryption.



# Symmetric key Distribution

Requires each pair of communicating parties to share a (separate) secret key.



# Last lecture: Public-Key Cryptography

Separate keys are used for encryption and decryption.



# **Public Distribution**

Only one key is needed for each recipient



# **Digital Signatures**

Public-key encryption provides a method for doing digital signatures

To sign a message, M,

• Alice just encrypts it with her private key, SA, creating  $C = E_{SA}(M)$ .

Anyone can decrypt this message using Alice's public key,

•  $M' = D_{PA}(C)$ , and compare that to the message M.

# **Cryptographic Hash Functions**

A checksum on a message, M, that is:

One-way:

- it should be easy to compute Y=H(M),
- but hard to find M given only Y

Collision-resistant:

• it should be hard to find two messages, M and N, such that H(M)=H(N).

Examples: SHA-1, SHA-256.

### Message Authentication Codes



# **Digital Certificates**

certificate authority (CA) digitally signs a binding between an identity and the public key for that identity.

#### Certificate Viewer:"www.cerias.purdue.edu"

#### General Details

This certificate has been verified for the following uses:

SSL Server Certificate

#### **Issued** To

Common Name (CN) Organization (O) Organizational Unit (OU)	www.cerias.purdue.edu Purdue University CERIAS
Serial Number	5E(9E(88)BF(B3(52)77)BU(A8(62)9U(7B)FF(FC(5F)C6
Issued By Common Name (CN) Organization (O) Organizational Unit (OU)	Thawte Premium Server CA Thawte Consulting cc Certification Services Division
Validity	
Issued On	6/3/2010
Expires On	6/4/2011
Fingerprints SHA1 Fingerprint MD5 Fingerprint	E1:2A:8A:25:FB:A1:CA:22:A0:6C:92:CC:92:49:E7:B8:1B:A1:84:69 2B:07:A4:C8:5B:8D:BA:01:9B:47:55:84:A4:C6:6E:7C
	⊆lose

#### Passwords

A short sequence of characters used as a means to authenticate someone via a secret that they know.

Userid:

Password:

#### What is a strong password

- UPPER/lower case characters
- Special characters
- Numbers

When is a password strong?

Seattle1

M1ke03

P@\$\$w0rd

TD2k5secV

### Password complexity

#### Odd characters make pass strong

A fixed 6 symbols password:

- Numbers
  - $\circ$  10<sup>6</sup> = 1,000,000
- UPPER or lower case characters
  - $\circ$  26<sup>6</sup> = 308,915,776
- UPPER and lower case characters
  - $\circ$  52<sup>6</sup> = 19,770,609,664
- 32 special characters
  - (&, %, \$, £, ", |, ^, §, etc.)
  - $\circ$  32<sup>6</sup> = 1,073,741,824

#### 94 practical symbols available

•  $94^6 = 689,869,781,056$ 

ASCII standard 7 bit 2<sup>7</sup> =128 symbols

•  $128^6 = 4,398,046,511,104$ 

#### Password length

- 5 characters: 94<sup>5</sup> =
- 6 characters: 94<sup>6</sup> =
- 7 characters: 94<sup>7</sup> =
- 8 characters: 94<sup>8</sup> =
- 9 characters: 94<sup>9</sup> =

7,339,040,224 689,869,781,056 64,847,759,419,264 6,095,689,385,410,816 572,994,802,228,616,704

### Password Validity: Brute Force Test

Password does not change for 60 days

how many passwords should I try for each second?

 5 characters:
 1,415 PW /sec

 6 characters:
 133,076 PW /sec

 7 characters:
 12,509,214 PW /sec

 8 characters:
 1,175,866,008 PW /sec

 9 characters:
 110,531,404,750 PW /sec

# Secure Passwords

A strong password includes characters from at least three of the following groups:

Group	Example
Lowercase letters	a, b, c,
Uppercase letters	A, B, C,
Numerals	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Non-alphanumeric (symbols)	( ) ` ~ ! @ # \$ % ^ & * - + =   \ { } [ ] : ; " ' < > , . ? /
Unicode characters	€, $\Gamma$ , $f$ , and $\lambda$

eg. "I re@lly want to buy 11 Dogs!"

How a password is stored?



- ★ Add "salt" to avoid the same password being encrypted to the same value
  - H(dog124+salt)
  - Save salt+ h(dog124+salt)

https://ics.uci.edu/~goodrich/teach/cs201P/notes/Ch01-Introdu ction.pdf



https://en.wikipedia.org/wiki/Salt (cryptography)

### Malware (malicious software)

#### A virus

It replicates itself:

- modifies other programs
- and inserts its own code into those programs

#### A worm

It actively transmits itself over a network to infect other computers and can copy itself without infecting files.

#### I'M THE CREEPER : CATCH ME IF YOU CAN!

**Creeper** was the first <u>computer worm</u>, while **Reaper** was the first <u>antivirus</u> software, designed to eliminate Creeper.

https://en.wikipedia.org/wiki/Creeper\_and\_Reaper

#### Trojan horse

A Trojan horse misrepresents itself to masquerade as a regular, benign program or utility in order to persuade a victim to install it

<u>Droppers</u> are a sub-type of Trojans that solely aim to deliver malware upon the system that they infect with the desire to subvert detection through stealth and a light payload

#### Spyware

Programs designed to monitor users' web browsing, display <u>unsolicited advertisements</u>, or redirect <u>affiliate marketing</u> revenues are called <u>spyware</u>.

Spyware programs do not spread like viruses; instead they are generally installed by exploiting security holes.

They can also be hidden and packaged together with unrelated user-installed software.

#### Ransomware

Ransomware prevents a user from accessing their files until a ransom is paid.

#### **Rootkits**

Once malicious software is installed on a system, it is essential that it stays concealed, to avoid detection.

Software packages known as rootkits allow this concealment, by modifying the host's operating system so that the malware is hidden from the user.

Rootkits can prevent a harmful process from being visible in the system's list of processes, or keep its files from being read.

# Vocabulary

Bug - An error only exist in source code

• When noticed easily correctable

**Flaw** - An error in the understanding or particularly in the design

• difficult and costly to correct

https://cs116.org

# Vulnerability

#### A vulnerability is

- a weakness,
- flaw
- or software bug

#### A vulnerability can be in

- an application
- a complete computer,
- an operating system,
- or a computer network that is exploited by malware to bypass defences or gain privileges it requires to run.

Common Vulnerabilities and Exposures

CVE created in 1999

Does NOT provide proof of concept (PoC) or exploit!

Common Weakness Enumeration

Common Weakness Enumeration Some vulnerabilities and proof of concepts

- <u>https://www.metasploit.com/</u>
- <u>https://www.exploit-db.com/</u>
- <u>https://cxsecurity.com/</u>
- <u>https://packetstorm.news/</u>
- Vx Underground
- <u>https://www.seebug.org/</u>

To search vulnerabilities in network and lot devices

- <u>ZoomEye</u>
- <u>Shodan</u>
- <u>CVE Search Engine Security</u>
   <u>Vulnerabilities and Exploits Search Tool</u>

### Reminder: Computer networks



#### Network Topology







### Packet and protocols (encapsulation)



A packet contains implementation of used protocols in every layer

• Source&destination IP, port numbers, MAC address, TCP, HTTPS etc.

Address Resolution Protocol (ARP)

- IPv4 address
- + MAC address (medium access control address)
  - A unique identifier assigned to network interface card (NIC) for communications at the data link layer of a network segment

Address Resolution Protocol -Wikipedia

# **Tool wireshark**

A popular network protocol analyzer

https://www.wireshark.org/

Wireshark captures packets and lets you examine their contents.

FI FID 10 - C				- 0
rile Edit View Go Capture Anal	yze Statistics Telepho	ny Wirele	ss Tools Help	
🕻 🔳 🦪 📵 📙 🖻 🗙 🖨 🔍 🤄	> + * * T & 🔁	. €	0. 1	
Apply a display filter <ctrl-></ctrl->				Expression.
The Course	Darkarkar	Dustand	Levelle Tele	
5. Time Source	Destination	Protocol	Length Into	Gen 1 Anh 1 Min 5999 Len 0 Tourl 401510346 Tourn 551911937
343 65.142415 192.168.0.21	174.129.249.228	TCP	66 40555 → 80 [ACK]	Seq=1 ACK=1 W1n=5888 Len=0 (SV81=491519346 (Secr=55181182/
344 65.142715 192.168.0.21	1/4.129.249.220	TCD	255 del /clients/neti	11X/11ash/application.swifflash_version=flash_lite_2.1&v=1.5
345 65 240742 174 129 249 220	102.100.0.21	HTTD	00 00 → 40555 [ACK]	d Temperateiju
346 63.240742 174.129.249.220	174 100 040 000	TCD	626 HTTP/1.1 302 MOVE	G TEMPORATILY
347 05.241592 192.100.0.21	1/4.129.249.220	DNC	00 40555 4 00 [ACK]	2100 A ada 0 afluing and
240 65.242332 192.100.0.21	192.100.0.1	DNS	490 Standard query 65	company a con-o.niiximg.com
549 65.276676 192.166.0.1	62 20 242 42	TCD	74 27062 Sea [SVAI]	Sponse 0x2188 A cun-0.111ximg.com charte images.netriix.com.e
251 65 207757 62 90 242 49	102 168 0 21	TCD	74 57005 4 00 [51N]	ACK 2 Sec-0 Ack-1 Mar-5702 Lon-0 MSS-1460 SACK DEDM-1 TSV01-491319402 13
351 05.257737 05.00.242.40	63 80 242 48	TCP	66 37063 - 80 [ACK]	Ack j Seq-0 Ack-1 Win-5752 Len-0 755-1400 SAck_FEM-1 15V01-
352 65 209697 102 169 0 21	63 90 242.40	NTTD	153 GET /us/psd/cliar	+r/flack/214540 hum WTTD/1 1
354 65 318730 63 80 242 48	192 168 0 21	TCP	66 80 + 37063 [ACK]	Sen=1 Ack=88 Win=5702 Len=0 TSval=3205534151 TSecr=401510503
355 65 321733 63 89 242 48	192 168 0 21	TCP	1514 [TCP segment of a	reascential DDU1
555 05.521755 05.00.242.40	172.100.0.21	TCT.	1914 Fich BeBuche of a	r cussembled r boj
Domain Name System (response)				
Domain Name System (response) [Request In: 348] [Time: 0.034338000 seconds]				
Domain Name System (response) [Request In: 348] [Time: 0.034338000 seconds] Transaction ID: 0x2188				
Domain Name System (response) [Request In: 348] [Time: 0.034338000 seconds] Transaction ID: 0x2188 Elass: 0x8180 Standard quer	v response. No erro	c.		
Domain Name System (response) [Request In: 348] [Time: 0.034338000 seconds] Transaction ID: 0x2188 > Flags: 0x8180 Standard quer Questions: 1	y response, No erro	r		
Domain Name System (response) [Request In: 348] [Time: 0.034338000 seconds] Transaction ID: 0x2188 > Flags: 0x8180 Standard quer Questions: 1 Answer BRs: 4	y response, No erro	r		
Domain Name System (response) <u>[Request In: 348]</u> [Time: 0.834338000 seconds] Transaction ID: 0x2188 > Flags: 0x6180 Standard quer Questions: 1 Answer RRs: 4 Authority RRs: 9	y response, No erro	r		
Domain Name System (response) [Request In: 348] [Time: 0.834338000 seconds] Transaction ID: 0x2188 > Flags: 0x2180 Standard quer Questions: 1 Answer RRs: 4 Authority RRs: 9 Additional RRs: 9	y response, No erro	r		
Domain Name System (response) [Request In: 343] [Time: 0.63330000 seconds] Transaction ID: 0x2188 > Flags: 0x2180 Standard quer Questions: 1 Answer RRs: 4 Authority RRs: 9 Additional RRs: 9 Vouries	y response, No erro	C		
Domain Name System (response) [Request In: 148] [Time: 0.04338000 seconds] Transaction ID: 0x2188 > Flags: 0x8100 Standard quer Questions: 1 Answer RRs: 4 Authority RRs: 9 Additional RRs: 9 > Queries > cdn-0.nflxing.com: type	y response, No erro A, class IN	C		
Domain Name System (response) [Request In: 348] [Time: 0.04338000 seconds] Transaction ID: 0x2188 > Flag: 0x43800 Standard quer Questions: 1 Antwer RRs: 4 Authority RRs: 9 Additional RRs: 9 > Queries > cdn-0.nflximg.com: type > Answer	y response, No erro A, class IN	r		
Domain Name System (response) [Request In: 343] [Time: 0.69338000 seconds] Transaction ID: 0x2188 > Flag: 0x2180 Standard quer Questions: 1 Answer RRs: 4 Authority RRs: 9 Additional RRs: 9 Y Queries > cdn-0.nflximg.com: type > Answers > Authoritative nameservers	y response, No erro A, class IN	r		
Domain Name System (response) [Request In: 148] [Time: 0.034330800 seconds] Transaction ID: 0x2188 > Flags: 0x0180 Standard quer Questions: 1 Answer RKs: 4 Authority RKs: 9 Additional RKs: 9 > cdn-0.nflximg.com: type > Answers > duthoritative nameservers 0 doi:10.05.05.45.47.47.77	y response, No erro A, class IN	01	5 20	
Domain Name System (response) [Request In: 348] [Time: 0.63330000 seconds] Transaction ID: 0x2188 > Flag: 0x3180 Standard quer Questions: 1 Answer RKs: 4 Authority RRs: 9 > Additional RRs: 9 > Queries > cdn-0.nflximg.com: type > Answer RS: 4 Authoritative nameservers 20 00 015 00 35 84 fel 01 c7 8 20 00 02 00 00 00 00 00 c5 6 7 6 7	y response, No erro A, class IN 3 3f <mark>21 85</mark> 81 80 00	n 01	5	
Domain Hame System (response) [Request In: 145] [Time: 0.34338000 seconds] Transaction ID: bx2188 > Flag: 0x8180 Standard quer Questions: 1 Answer RRs: 4 Authority RRs: 9 Additional RRs: 9 > don-0.nfiximg.com: type > Answers ≥ 0.00 -0.07 stateservers 200 00 15 00 35 84 F4 01 c7 8 00 04 00 09 06 00 05 63 6 78 69 64 67 08 55 66 d	y response, No erro A, class IN 3 37 21 80 51 80 00 4 6c 2d 30 97 6c 66 0 60 10 00 1 c0 0c	01 6c 00 xim	5	
Domain Hame System (response) [Raquest In: 348]           [Time: 0.83433800 seconds]           Transaction 10: 0x2188           > Flag: 0x8180 standard quer Questions: 1           Answer RS: 4           Authority RRs: 9           > duditional RRs: 9           > Queries           > Answer Rs: 4           Authority RRs: 9           > duditional RRs: 9           > Queries           > Answer Rs: 4           Authority RRs: 9           > Authoritative nameservers           020 00 50 00 90 00 90 50 56 35           000 60 00 90 90 90 53 56 65 do           000 65 00 00 00 90 90 90 53 56 65 do           000 85 00 01 00 00 65 20 90 22	y response, No erro A, class IN 3 3f 21 86 81 80 00 4 6e 2d 30 07 6e 66 0 00 01 00 01 c0 0c 0 06 90 60 16 7 65	01 6c 00 xim 73	5	
Domain Name System (response) [Request In: 343] [Time: 0.84338000 seconds] Transaction ID: 0x2188           > Flags: 0x8180 Standard quer Questions: 1 Answer RRs: 4 Authority RRs: 9 > dditional RRs: 9 > Queries > cdn.0.nflximg.com: type > Answers           > Cdn.0.nflximg.com: type > Answers           > Authority nameservers           200         00 15 00 35 44 f4 01 c7 7 08 00 46 00 00 00 65 25 00 7 66 55 74 65 66 c7 97 8 00	A, class IN 3 3f 21 86 81 80 00 4 6e 2d 30 07 6e 66 0 00 01 00 1c 0 0c 2 06 69 6d 01 c0 76 2 06 69 6d 91 c6 76	01 6c 00 xim 73 67 .ne	5	
Domain Hame System (response) [Request In: 348] [Time: 0.03433000 seconds] Transaction ID: 0x2188           > Flags: 0x8100 Standard quer Questions: 1 Answer RRs: 4 Authority RRs: 9 Additional RRs: 9           > Queries > con-0.nflximg.com: type > Authoritative nameservers           20         00 15 00 35 44 f4 01 c7 3 00 45 00 68 26 00 62 3 00 46 00 60 60 60 60 60 86 60 01 60 60 36 66 60 86 86 00 10 60 60 56 87 6 86 57 37 56 57 46 58 36 66	y response, No erro A, class IN 3 3f <u>31 60</u> 81 80 00 4 6e 2d 30 07 6e 6 0 00 10 00 10 c0 00 3 66 61 67 65 3 63 6f 6d 90 657 65 3 63 6f 6d 90 657 65 3 63 6f 6d 90 657 65	01 06 00 xim 73 67 .ne 00 esu	5 ≹ c dn-0.nfl .com filcom.edg filcom.edg teet	

https://www.wireshark.org/docs/wsug\_html\_chunked/ChapterIntroduction.html#ChIntroPurposes

### Attacking networks: network sniffing

Look at network traffic

Most of the traffic on a network is still unencrypted, plaintext ("in the clear")



Things you can do with network sniffing:

- Troubleshoot networking issues
- Record communications (e.g., email, voice, chat)
- Catch usernames and passwords, personal information, and other sensitive information

Image source: <u>https://www.avast.com/c-packet-sniffing</u> <u>https://cs116.org/slides/03\_attacking\_networks.pdf</u>

# Network sniffing tools

#### Ettercap and :: bettercap

Is not intended for network traffic analysis but has capabilities for:

- Capturing passwords
- Conducting man-in-the-middle (eavesdropping) attacks
- Hijacking sessions

#### dsniff | Kali Linux Tools

Suite of networking sniffing tools including

- dsniff password sniffer
- webspy intercepts URLs entered
- mailsnarf intercepts POP or SMTP-based mail

# How to prevent network sniffing

Use encryption and encrypted network protocols

E.g.

- Use HTTPS instead of HTTP
- Use SSH instead of RSH or Telnet
- Use SCP instead of FTP
- Use IMAP or POP3 over SSL
- Use a Virtual Private Network (VPN)

#### Attacking networks: Network Scanning

Why? Network reconnaissance. Warfare 101

- What devices and computers are up?
- What ports are open on a computer?
- What services are running?
- Determine possible vulnerabilities?
- Still extremely relevant today
- Think poking holes, "ask questions"
- Poking holes: finding interesting and unwanted stuff on networks

Zoomeye and shodan can be used for this purpose

Fping: fping man-page,

Nmap: <u>Chapter 15. Nmap Reference Guide |</u> <u>Nmap Network Scanning</u>

Netcat: nc(1): arbitrary TCP/UDP connections/listens - Linux man page

Shodan: Shodan

Zoomeye: ZoomEye

#### Attacking networks: Distributed Denial of Service (DDoS) Attacks

The idea: to make a resource unavailable (the "A" in the CIA Triad) using many remote computing devices.

That is, overwhelm or flood a target (e.g., with so much network traffic)

• Imagine if an important service you use like Gmail, Google, Netflix, Twitter, GitHub is down

- Terabit scale Distributed Denial of Service (DDoS) attacks from September 2016 to late 2016
- How: using thousands of infected devices, mostly cameras. Devices infected via weak username:password hardcoded on device (e.g.,root:root, admin:admin)
- Results: took down Brian Kreb's blog in September 2016; GitHub, Twitter, Netflix, and many major services were affected via DDoS on Dyn DNS in October 2016 (i.e., "all eggs in one basket")
- Source code of Mirai botnet: <u>GitHub -</u> jgamblin/Mirai-Source-Code
- Rob Graham's presentation on "Mirai and IoT Botnet Analysis" at RSA Conference 2017:
- <u>https://vinceinthebay.files.wordpress.com/20</u>
   <u>17/02/rsac-slides-hta-w10-mirai-1.pdf</u>

# DDOS flood Types

SYN Flood

• exhaust states in the TCP/IP stack

Ping of death

• violate the IP contract, send large packets to cause unexpected errors

And many others



# **Remember URL**

Example: https://www.google.com/search?q=grand+theft+auto&lr=lang\_zh-TW

(returns Google results on "Grand Theft Auto" in Chinese Traditional language)

- q => Google's key in query string for "query"
- Ir => Google's key in query string for "language"

Notice example URL uses https. That is HTTP + Transport Layer Security (TLS)

# **HTTP Request**

#### header

- GET Download data from server.
  - This is always the HTTP command used when you type in a URL into address bar
- POST Sent to server from a form
- PUT Upload
- DELETE

Additional HTTP commands: HTTP - Wikipedia

#### body

data to be sent to server including **query string key-value pairs** 

### **HTTP** response

#### header

- 200 OK
- 301 Moved Permanently
- 302 Found (the request was redirected to another URL/URI)
- 401 Unauthorized
- 403 Forbidden
- 404 Not Found
- 500 Internal Server Error

#### body

the content data (e.g., HTML, text, JSON, etc.)

#### Web security

The Open Worldwide Application Security Project (OWASP) <u>OWASP Foundation</u> is a nonprofit foundation that works to improve the security of software. Our programming includes:

- Community-led open source projects including code, documentation, and standards
- Over 250+ local chapters worldwide
- Tens of thousands of members
- Industry-leading educational and training conferences

#### OWASP Top 10 Web Application Security Risks

#### 2017

A01:2017-Injection A02:2017-Broken Authentication A03:2017-Sensitive Data Exposure A04:2017-XML External Entities (XXE) A05:2017-Broken Access Control A06:2017-Security Misconfiguration A07:2017-Cross-Site Scripting (XSS) A08:2017-Insecure Deserialization A09:2017-Using Components with Known Vulnerabilities A10:2017-Insufficient Logging & Monitoring 2021 A01:2021-Broken Access Control A02:2021-Cryptographic Failures A03:2021-Injection (New) A04:2021-Insecure Design A05:2021-Security Misconfiguration A06:2021-Vulnerable and Outdated Components A07:2021-Identification and Authentication Failures (New) A08:2021-Software and Data Integrity Failures A09:2021-Security Logging and Monitoring Failures\* (New) A10:2021-Server-Side Request Forgery (SSRF)\* \* From the Survey

#### OWASP Top Ten

	<u>2024</u>	<u>CWE</u>	Гор
--	-------------	------------	-----

<u>25 Most</u>

**Dangerous** 

<u>Software</u>

<u>Weaknesses</u>

Rank	ID	Name		CVEs in KEV	Rank Change vs. 2023
1	<u>CWE-79</u>	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	56.92	3	+1
2	<u>CWE-787</u>	Out-of-bounds Write	45.20	18	-1
3	<u>CWE-89</u>	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	35.88	4	0
4	CWE-352	Cross-Site Request Forgery (CSRF)	19.57	0	+5
5	<u>CWE-22</u>	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12.74	4	+3
6	<u>CWE-125</u>	Out-of-bounds Read	11.42	3	+1
7	<u>CWE-78</u>	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11.30	5	-2
8	<u>CWE-416</u>	Use After Free		5	-4
9	CWE-862	Missing Authorization		0	+2
10	<u>CWE-434</u>	Unrestricted Upload of File with Dangerous Type		0	0
11	<u>CWE-94</u>	Improper Control of Generation of Code ('Code Injection')		7	+12
12	<u>CWE-20</u>	Improper Input Validation		1	-6
13	<u>CWE-77</u>	Improper Neutralization of Special Elements used in a Command ('Command Injection')		4	+3
14	<u>CWE-287</u>	Improper Authentication	5.94	4	-1
15	<u>CWE-269</u>	Improper Privilege Management	5.22	0	+7
16	<u>CWE-502</u>	Deserialization of Untrusted Data	5.07	5	-1
17	<u>CWE-200</u>	Exposure of Sensitive Information to an Unauthorized Actor		0	+13
18	CWE-863	Incorrect Authorization		2	+6
19	CWE-918	Server-Side Request Forgery (SSRF)		2	0
20	<u>CWE-119</u>	Improper Restriction of Operations within the Bounds of a Memory Buffer		2	-3
21	<u>CWE-476</u>	NULL Pointer Dereference		0	-9
22	<u>CWE-798</u>	Use of Hard-coded Credentials	3.46	2	-4
23	<u>CWE-190</u>	Integer Overflow or Wraparound			-9
24	<u>CWE-400</u>	Uncontrolled Resource Consumption Notice the similarities with	n the		+13
25	<u>CWE-306</u>	Missing Authentication for Critical Function OWASP Top 10 list			-5

https://cs116.org/slides/06\_web\_security.pdf

2024 CWE Top 25

# Is There a Legal Way or Place to Practice Attacking Web Applications?

# IMPORTANT: NEVER DEPLOY THESE WEB APPLICATIONS TO THE PUBLIC INTERNET OR ON A PRODUCTION SYSTEM!

- Damn Vulnerable Web Application (DVWA) http://www.dvwa.co.uk/
- Mutillidae <u>https://sourceforge.net/projects/mutillidae/</u>

• Hacme Casino - <u>https://www.mcafee.com/us/downloads/freetools/hacme-casino.aspx</u> (old; Ruby on Rails based)

- WebGoat https://github.com/WebGoat/WebGoat/wiki ; by OWASP
- A plethora deliberately vulnerable web applications to install and practice on

# Metasploitable 2

An intentionally vulnerable Linux virtual machine (VM)

https://sourceforge.net/projects/metasploitable/

- Uses VMware by default; can run on VirtualBox
- Contains Damn Vulnerable Web Application, Mutillidae, phpMyAdmin, etc.
- Great practice environment
- References:
- <u>https://community.rapid7.com/docs/DOC-1875</u>
- <u>https://www.offensive-security.com/metasploit-unleashed/requirements/</u>

# Some other tools

A web proxy will be an important tool for testing and breaking web applications

Many web proxie software available:

- Burp Suite
- OWASP Zed Attack Proxy (ZAP)
- Tamper Data for Firefox
- mitmproxy

# The vulnerabilities

The Principle of Least Privilege –Or Lack thereof

• The issue1: connecting to a database or system as root or as administrator -- which has the power to do anything

#### Hard-Coded Credentials

- The issue2: username and password or key are hard-coded in source code
- God forbid if you push source code with the credentials to GitHub

#### 

### cross-site scripting (XSS)



https://portswigger.net/web-security/cross-site-scripting, attacker's script executes in the user's browser

# **SQL** Injection

' UNION SELECT username, password FROM users--



https://portswigger.net/web-security/sql-injection

# End of semester