Welcome Cyber#1

Reader: reader.codaisseur.com

Slack: codaisseur-school.slack.com

Discord: https://discord.gg/qyehPh

WEB ATTACKs

Today...

- Web Attacks & statistics
- Brute force
- SQL Injection
- XSS Attacks
- Command injections
- PlayTime

Numbers

+/- x%

Link

Attacks in 2020...

70% increase in overall attack volume.

- Application-specific (31%)
- DDoS (25%) attacks

Attacks in 2020...

70% increase in overall attack volume.
- Application-specific (31%)
- DDoS (25%) attacks

Governments see a 200% increase in attack volume

Web Attacks in 2020...

47% of all hacked websites contained at least one backdoor.

SENHA

password	Users
123456	2,543,285
123456789	961,435
picture1	371,612
password	360,467
12345678	322,187
111111	230,507
123123	189,327
12345	188,268
1234567890	171,724
senha	167,728

During our coding bootcamp..

Web Attacks in 2020...

4.2 billion web application attacks were blocked in Q1+Q2

Web Attacks in 2020...

42% SQL injections
19% XSS
16% PHP
7% RCE (Remote code execution)
16% other

WHY???

86% of breaches were financially motivated
10% were motivated by espionage

Numbers from...

Numbers from...

Verizon
symantec
Cisco
DELL
A&T
Google

McAfee
IBM
Intel
Fortinet
FireEye
...

Brute force...


#CHICAGOPD
NBC

An estimated 300 billion passwords are used by humans and machines worldwide.

admin : admin

admin : 12345678

SQL Injections

```
SELECT * FROM users WHERE email =
"jeroen@codaisseur.com" AND password = "ABCDEF";
```

Fun!...

```
SELECT * FROM users WHERE email =
"jeroen@codaisseur.com" AND password = "ABCDEF
                " or "1"="1   ";
```

Harmful...

SELECT * FROM users WHERE email = "jeroen@codaisseur.com" AND password = "ABCDEF "; DROP TABLE users; -- " ;

How to prevent?
SQL Injections

Better...

Mysql_real_escape_string
Removes:

```
// Escape special characters, if any
$firstname = $mysqli -> real_escape_string($_POST['firstname']);
$lastname = $mysqli -> real_escape_string($_POST['lastname']);
$age = $mysqli -> real_escape_string($_POST['age']);

$sql="INSERT INTO Persons (FirstName, LastName, Age) VALUES ('$firstname', '$lastname', '$age')";
```

Solution...

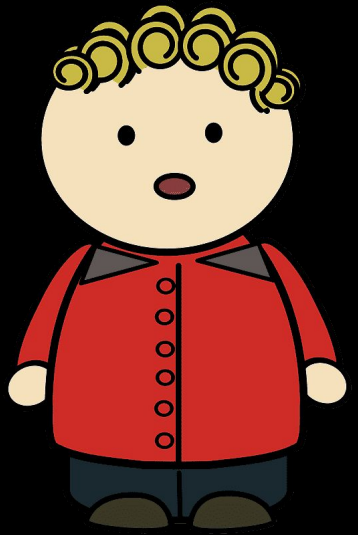
Prepared statements

https://www.w3schools.com/php/php_mysql_prepared_statements.asp

Harmful...

https://stackoverflow.com/questions/5741187/sql-injection-that-gets-around-mysql-real-escape-string

XSS Attacks



Harry

facebook.com

Apps | public-apis/public... | HAT / Addon Boar... | IO Pi Plus - 32 Ch... | React App | drstxz | Rendang recepten... | MockFlow - Onlin... | 90 | Heibaservice Portal | Redux, Redux, Re... | React App | UniFi Video | f | FFmpeg Filters Do...

Search Facebook

Jeroen

Jeroen Bruinsma

COVID-19 Information Center

Friends
3 requests

Groups

Marketplace

Watch
9+ new videos

Events

Memories

Saved

See More

Your Shortcuts

Goooooon Group! Groovy Grape

Create a Story

CNET

MIT Technology Review

IFLScience

Word Porn

On The Tools

Jeroen, we're asking a small group of people for their opinion
Could you take a few minutes to answer a short survey?

Start Survey | Dismiss

What's on your mind, Jeroen?

Live Video | Photo/Video | Feeling/Activity

Create Room

What do you do if you're recovering from a concussion, bored out of you mind and can't watch the tv or listen to stuff? Yes! Watercolor painting!

Most of these are recreations of youtube tutorials and not created by my own mind. I

Sponsored

Northumbria University
northumbria.ac.uk

Your First Line of Defense Against Power Outages
indiegogo.com

Birthdays

Zachary Dexter-Stitz's birthday is today.

Contacts

Privacy · Terms · Advertising · Ad Choices · Cookies

https://www.facebook.com/Jeroenbruinsma/

facebook.com

Apps | public-apis/public... | HAT / Addon Boar... | IO Pi Plus - 32 Ch... | React App | drstxz | Rendang recepten... | MockFlow - Onlin... | 90 | Heibaservice Portal | Redux, Redux, Re... | React App | UniFi Video | f | FFmpeg Filters Do...

Search Facebook

Jeroen

Jeroen Bruinsma

COVID-19 Information Center

Friends
3 requests

Groups

Marketplace

Watch
9+ new videos

Events

Memories

Saved

See More

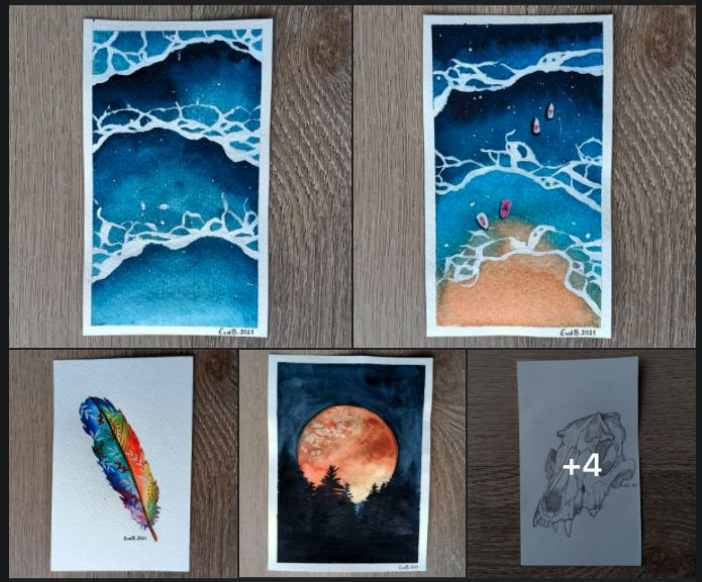
Your Shortcuts

Goooooon Group! Groovy Grape

Most of these are recreations of youtube tutorials and not created by my own mind. I copied/stole the outline and peeked at the finished product because you can't really watch them if you can't look at a screen🤣.

Enjoy!

P... See More



57

19 Comments

Like

Comment

Sponsored

Northumbria University
northumbria.ac.uk

Your First Line of Defense Against Power Outages
indiegogo.com

Birthdays

Zachary Dexter-Stitz's birthday is today.

Contacts

Privacy · Terms · Advertising · Ad Choices · Cookies

https://www.facebook.com/Jeroenbruinsma/

facebook.com

Apps | public-apis/public... | HAT / Addon Boar... | IO Pi Plus - 32 Ch... | React App | drstxz | Rendang recepten... | MockFlow - Onlin... | 90 | Heibaservice Portal | Redux, Redux, Re... | React App | UniFi Video | f | FFmpeg Filters Do...

Search Facebook

Jeroen

Jeroen Bruinsma

COVID-19 Information Center

Friends
3 requests

Groups

Marketplace

Watch
9+ new videos

Events

Memories

Saved

See More

Your Shortcuts

Goooooon Group! Groovy Grape

40

6 Comments

Like

Comment

Sponsored

Northumbria University
northumbria.ac.uk

Your First Line of Defense Against Power Outages
indiegogo.com

Birthdays

Zachary Dexter-Stitz's birthday is today.

Contacts

Privacy · Terms · Advertising · Ad Choices · Cookies

https://www.facebook.com/Jeroenbruinsma/

XSS

Fun...

```
<p>Cats are so cool <script>evil_script()</script>
```

Fun...

```
<b onmouseover="alert('Autch!')">click me!</<b>
```

Not so Fun...

```
<b onmouseover="alert(document.cookie)">click me!</<b>
```

Pro's doing XSS...

1. Load a script
2. <Wait>
3. Execute script (on click)
4. Send info to your server

Command injections

ifconfig <interface>

```
┌──(jeroen㉿kali01)-[~]
└─$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 104.248.193.148  netmask 255.255.240.0  broadcast 104.248.207.255
        inet6 fe80::1023:d6ff:fe02:3561  prefixlen 64  scopeid 0×20<link>
        ether 12:23:d6:02:35:61  txqueuelen 1000  (Ethernet)
        RX packets 1606843  bytes 511613760 (487.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1467741  bytes 2454651965 (2.2 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

ifconfig <interface> ; ls /

```
┌──(jeroen㉿kali01)-[~]
└─$ ifconfig eth0 ; ls /
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 104.248.193.148  netmask 255.255.240.0  broadcast 104.248.207.255
        inet6 fe80::1023:d6ff:fe02:3561  prefixlen 64  scopeid 0×20<link>
        ether 12:23:d6:02:35:61  txqueuelen 1000  (Ethernet)
        RX packets 1609421  bytes 511879071 (488.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1470215  bytes 2454962648 (2.2 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

bin   etc   index.html   initrd.img.old  lib64       media  proc  sbin  tmp  vmlinuz
boot  flag  index.html~  lib             libx32      mnt    root  srv   usr  vmlinuz.old
dev   home  initrd.img   lib32           lost+found  opt    run   sys   var
```

ifconfig <interface> ; dog /user/password

BurpSuite

WAIT!

Todo...

Many things -> see slack

PlayTime

LAB!

Groups

1. 10.110.0.14
2. 10.110.0.16
3. 10.110.0.17

Groups

1. Willemijn, Yvonne, Shangram,
2. Raj, Prwesh, Tjitze, Pepijn
3. Yann, Camilia, Ximena, Filipe

GO!