



(Ne)Sigurnost hrvatskog Internet prostora



OWASP

The Open Web Application Security Project



OWASP

The Open Web Application Security Project

- Marko Stanec
- Obrada računalnih incidenata
- Provjera ranjivosti
- Razvoj alata (Python/Django)





OWASP

The Open Web Application Security Project

- ✔ Uklanjanje malicioznog sadržaja s Interneta
- ✔ Obrada incidenata na Internetu, ako se jedna od strana u incidentu nalazi u RH, osim tijela državne uprave (ZSIS CERT)
- ✔ Diseminacija informacija (vijesti, preporuke, dokumenti, brošure, alati)
- ✔ Forenzika, analiza malvera, mrežnog prometa, logova...

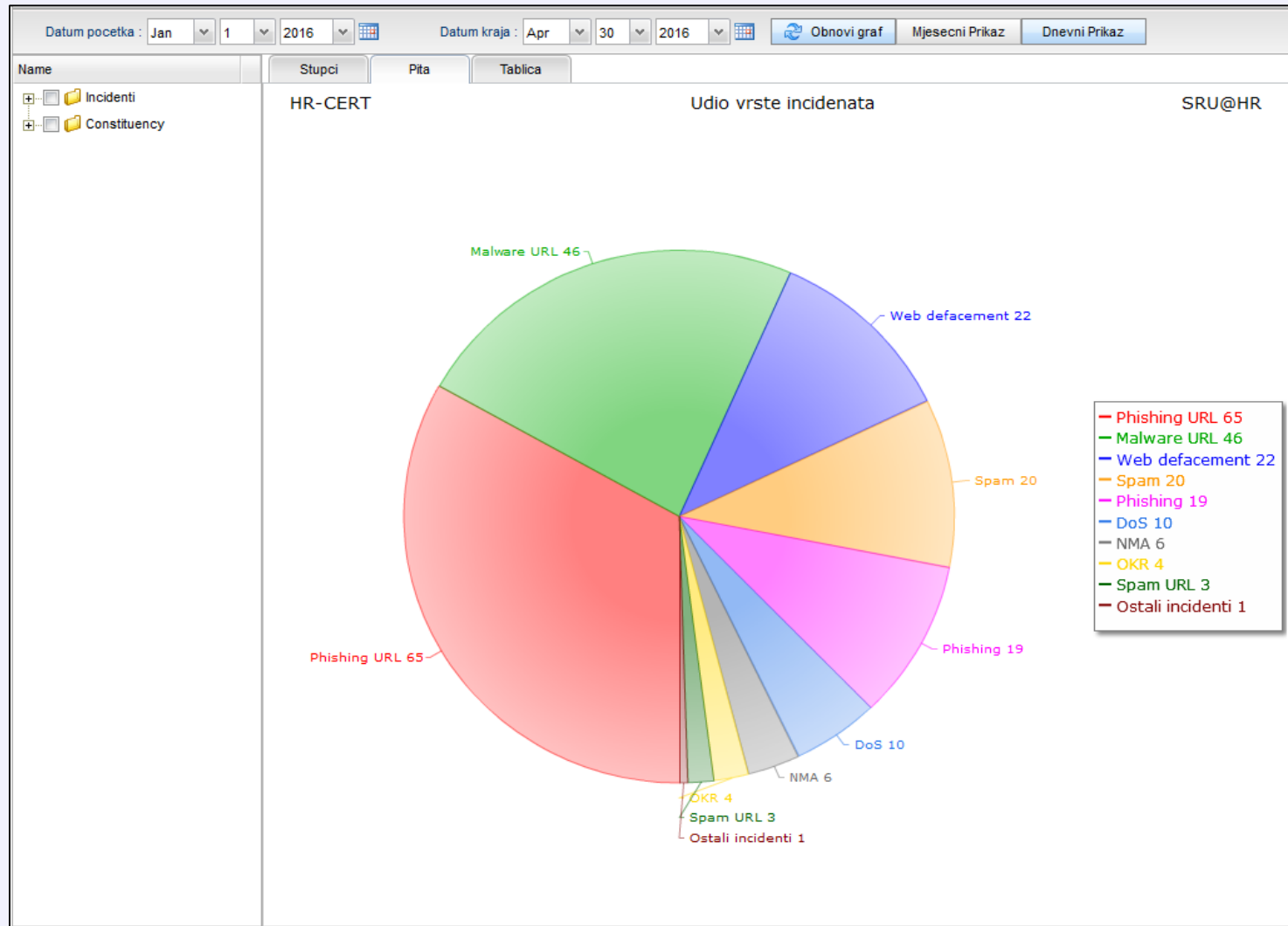
- ✘ operativno rješavanje problema i briga o sigurnosti pojedinih sustava
- ✘ kažnjavanje problematičnih korisnika
- ✘ arbitraža u sporovima
- ✘ pokretanje krivičnih prijava

SRU@HR – vrste incidenata



OWASP

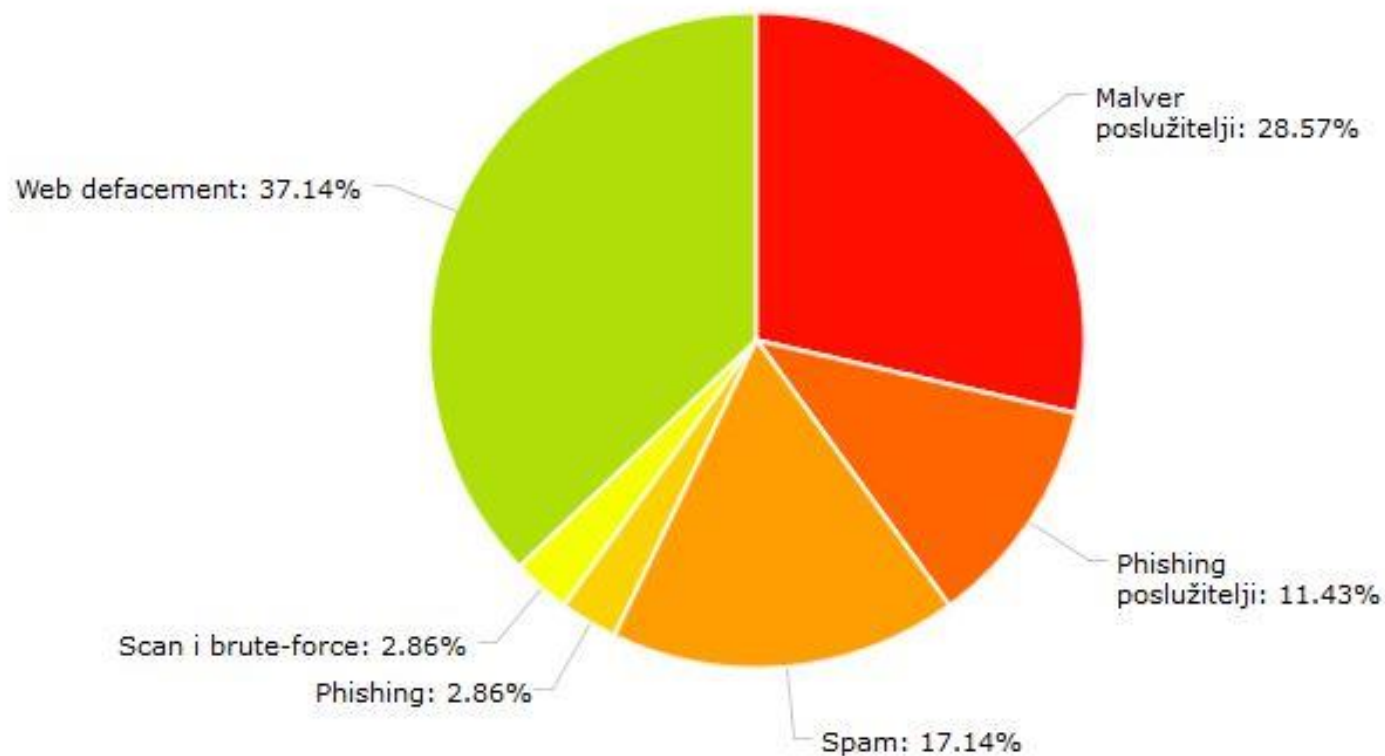
The Open Web Application Security Project





Obrađeni incidenti u zadnjih 30 dana

chart by amcharts.com



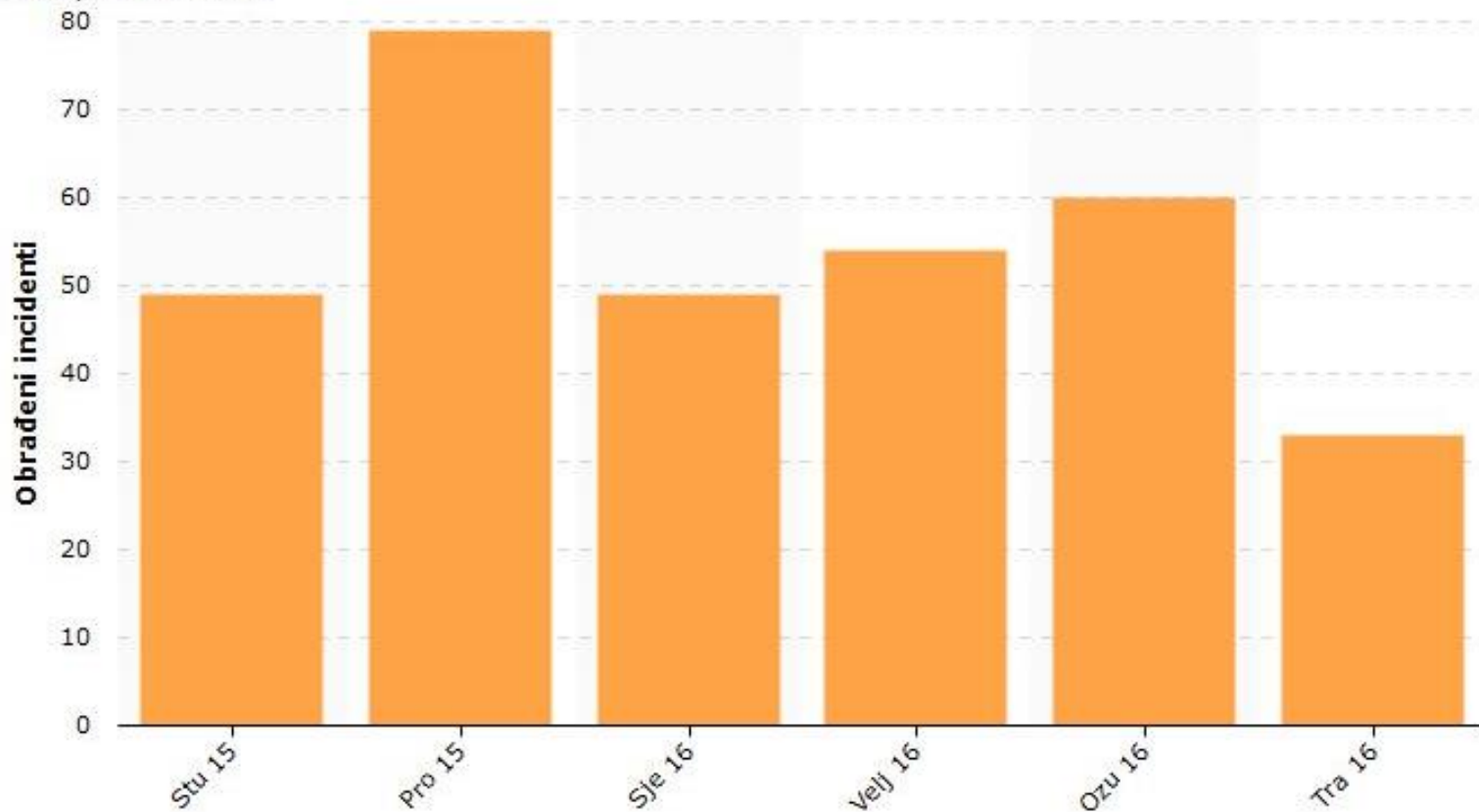


OWASP

The Open Web Application Security Project

Kretanje broja incidenata na poslužiteljima

chart by amcharts.com

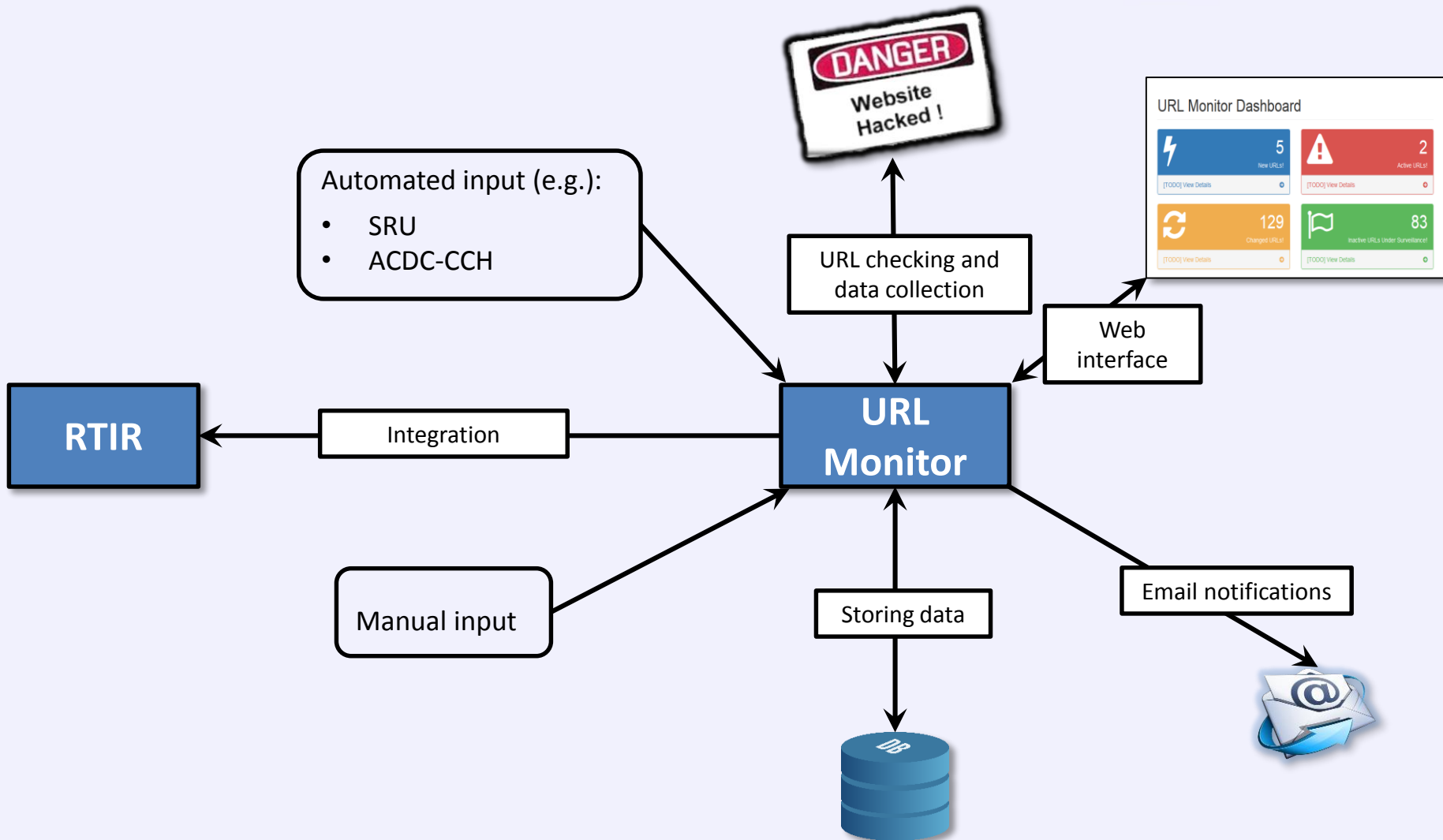


URL Monitor



OWASP

The Open Web Application Security Project



URL Monitor Dashboard



OWASP

The Open Web Application Security Project

URL Monitor beta

- Dashboard
- Monitored URLs
- Statistics

URL Monitor Dashboard

2 New URL's! [TODO] View Details

6 Active URL's! [TODO] View Details

4 Changed URL's! [TODO] View Details

10 Inactive URL's Under Surveillance! [TODO] View Details

Last URLs

URL	URL Type	State	Last Change
[REDACTED]	Web Defacement	NEW	4. svibnja 2016. 13:07
[REDACTED]	Web Defacement	ACTIVE	4. svibnja 2016. 12:40
[REDACTED]	Malware URL	NEW	4. svibnja 2016. 12:07
[REDACTED]	Phishing URL	ACTIVE	4. svibnja 2016. 04:40
[REDACTED]	Phishing URL	INACTIVE	3. svibnja 2016. 23:07
[REDACTED]	Phishing URL	INACTIVE	3. svibnja 2016. 23:07
[REDACTED]	Phishing URL	INACTIVE	3. svibnja 2016. 23:07
[REDACTED]	Malware URL	INACTIVE	3. svibnja 2016. 16:00
[REDACTED]	Malware URL	INACTIVE	3. svibnja 2016. 12:15
[REDACTED]	Malware URL	INACTIVE	3. svibnja 2016. 11:30

[View All URLs](#)

Notifications Panel

- New URL - [REDACTED] 4. svibnja 2016. 13:07
- Active URL - [REDACTED] 4. svibnja 2016. 12:40
- Inactive URL - [REDACTED] 4. svibnja 2016. 12:30
- New URL - [REDACTED] 4. svibnja 2016. 12:07
- Active URL - [REDACTED] 4. svibnja 2016. 04:40
- Inactive URL - [REDACTED] 4. svibnja 2016. 01:00
- Inactive URL - [REDACTED] 3. svibnja 2016. 23:07
- Inactive URL - [REDACTED] 3. svibnja 2016. 23:07
- Inactive URL - [REDACTED] 3. svibnja 2016. 23:07
- Active URL - [REDACTED] 3. svibnja 2016. 20:40

[\[TODO\] View All Events](#)

URL Types (last 15 days)

URL Type	Percentage
Web Defacement	46.34%
Malware URL	36.59%
Phishing URL	17.07%

URL Trend (last 15 days)

Date	Number of URLs
2016-04-19	1
2016-04-20	2
2016-04-21	13
2016-04-22	2
2016-04-23	1
2016-04-24	1
2016-04-25	1
2016-04-26	1
2016-04-27	1
2016-04-28	1
2016-04-29	1
2016-04-30	1
2016-05-01	5
2016-05-04	4

URL details



OWASP

The Open Web Application Security Project

URL Details

INACTIVE

URL: <input type="text"/>	IP Address: <input type="text"/>
URL Type: <input type="text" value="Phishing URL"/>	Domain: <input type="text"/>
Source: <input type="text" value="SRU"/>	DNS Data: <input type="text"/>
Frequency: <input type="text" value="60"/>	Redirect URL: <input type="text"/>
	Country Code: <input type="text" value="FR"/>
	Customer: <input type="text"/>
	Monitor Type: <input type="text" value="MD5 Hash"/>

Save Changes

URL log



OWASP

The Open Web Application Security Project

URL Log

Show 10 entries

Search:

State	Status Code	Screenshot	MD5 Hash	File Type	File	Last change	Actions
changed	200		7aeb47b912a8099048eef1239e74ff73	text/html		11/05/2016 - 00:40	
inactive	Unreachable					10/05/2016 - 20:45	
active	200		7aeb47b912a8099048eef1239e74ff73	text/html		04/05/2016 - 20:40	
inactive	Unreachable					04/05/2016 - 17:30	
active	200		7aeb47b912a8099048eef1239e74ff73	text/html		04/05/2016 - 04:40	
inactive	Unreachable					04/05/2016 - 01:00	
active	200		7aeb47b912a8099048eef1239e74ff73	text/html		03/05/2016 - 08:07	

Showing 1 to 7 of 7 entries

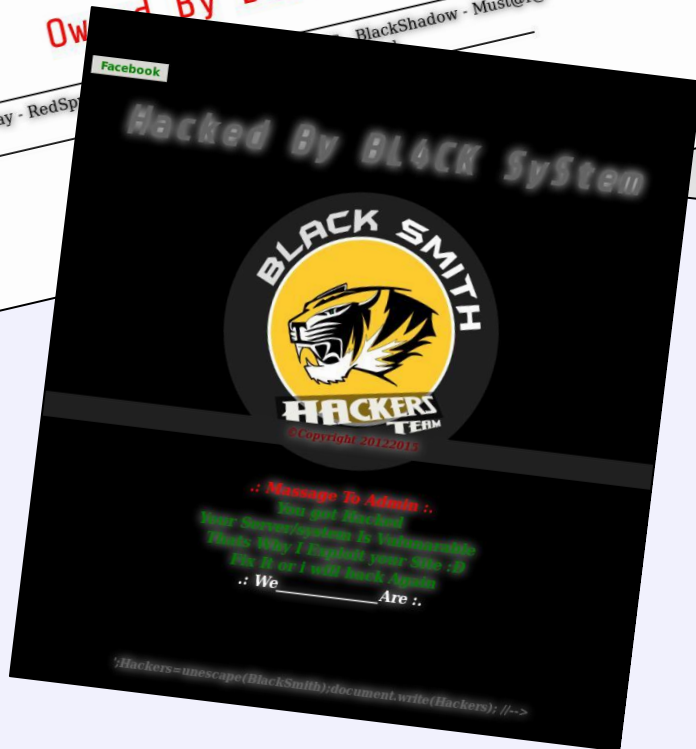
< Previous 1 Next >

Web defacements



OWASP

The Open Web Application Security Project



Phishing sites



OWASP

The Open Web Application Security Project

Alibaba.com English

Global trade starts here.™

Start your Trade on Alibaba.com

- ✓ 45 million members in 190+ countries
- ✓ Over 2 million supplier storefronts
- ✓ Safe and simple trade solutions

Email Address:

Email Password: [Forgot password?](#)

[Join free now!](#)

Google Drive

To view attached document you are required to Log in with your email address below

Email:

Password:

YAHOO! AOL Windows Live Gmail

Other emails

Google Drive

To view shared document, you are required to Login with your email address below.

Choose your email provider below and login:

YAHOO! Gmail

© Google - Privacy Policy - Help

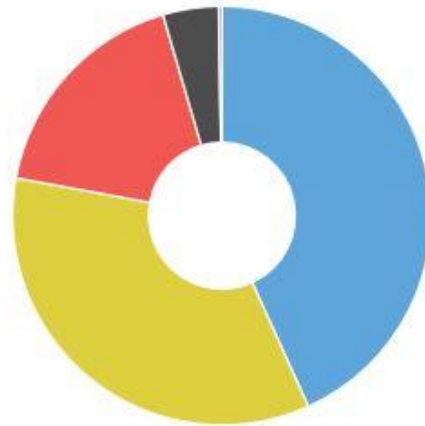
Slides



URL Type Distribution

URL Type Distribution

(01/01/2016 - 11/05/2016)



Phishing URL (43.24%)	Web Defacement (34.64%)
Malware URL (17.57%)	Unknown (4.3%)
Spam URL (0.25%)	

URL trend



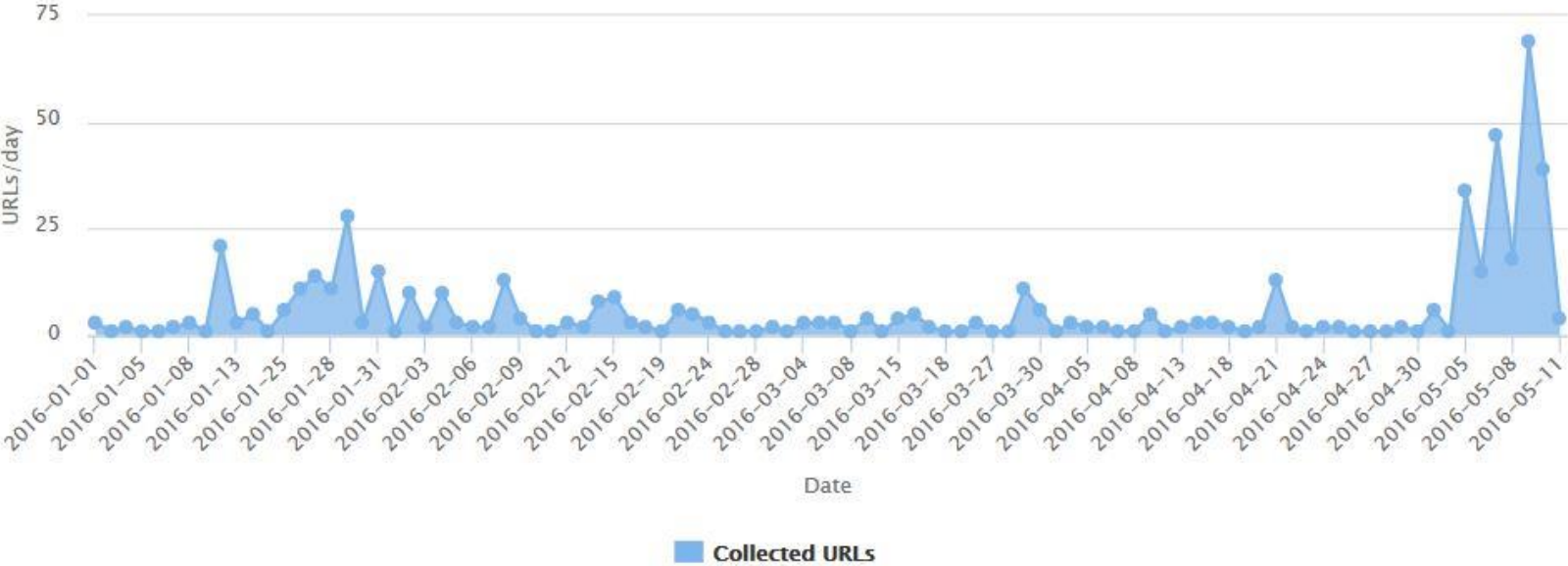
OWASP

The Open Web Application Security Project

URL Trend

URL Trend

(01/01/2016 - 11/05/2016)





- Služi za učenje, podučavanje i istraživanje
- Otvorenost – slabo postavljene sigurnosne mjere
- Veliki broj korisnika – učenici, studenti, nastavno osoblje, vanjski suradnici...
- Napredna računalno-komunikacijska tehnologija
- Veliki kapaciteti linkova



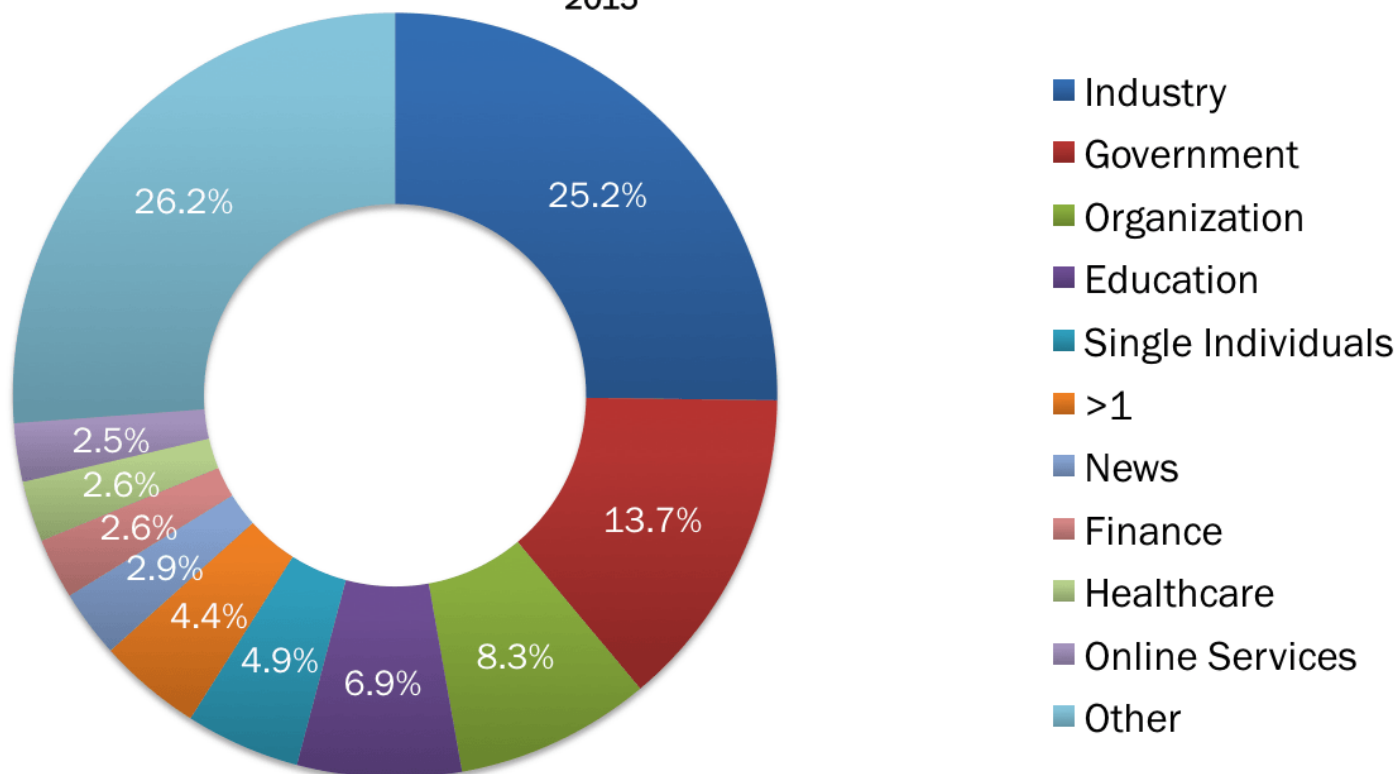
- Mreže obrazovnih i akademskih zajednica jedne od najzanimljivijih meta napada
- Prema raznim istraživanjima pri samom vrhu prema broju napada na internetu
- Najčešće nisu krajnji cilj
- Izvođenje daljnjih napada



OWASP

The Open Web Application Security Project

Top 10 Distribution of Targets 2015



(Izvor: www.hackmageddon.com)

SPORT



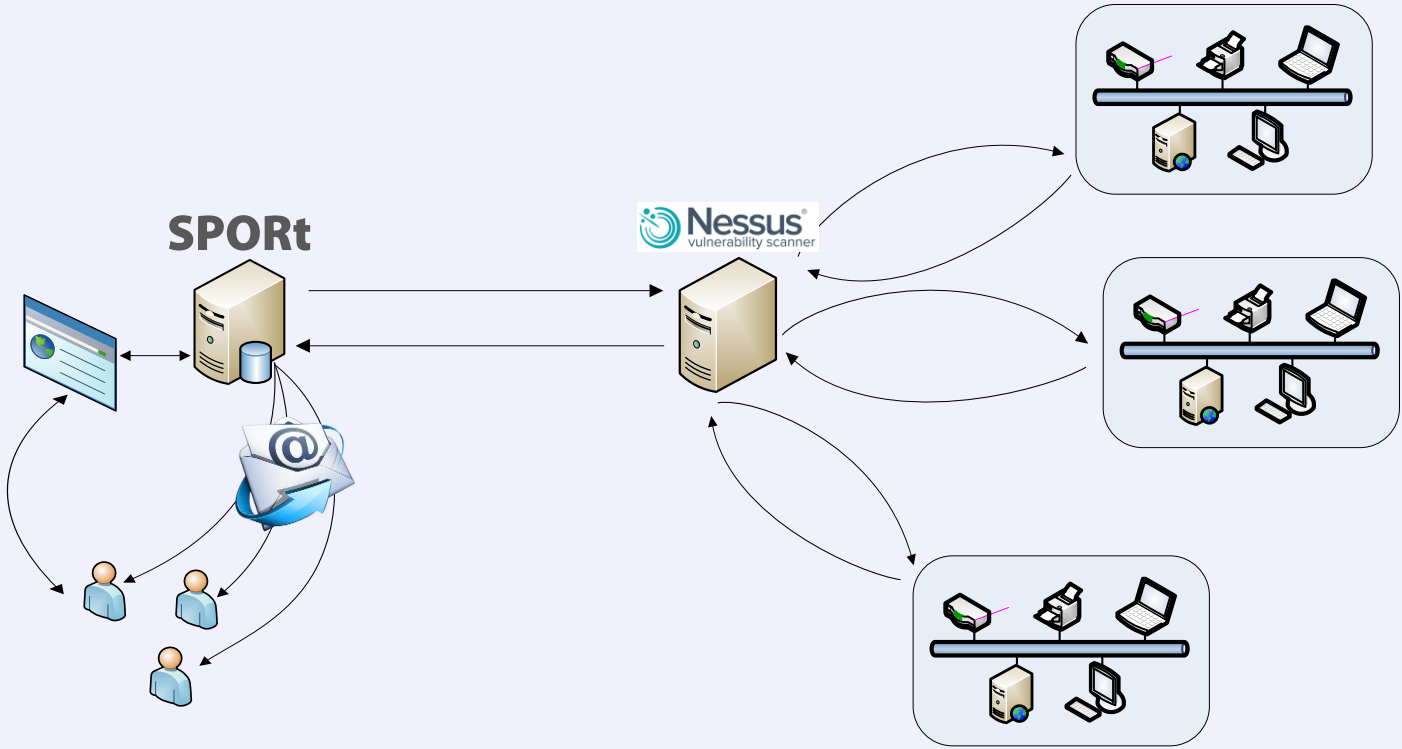
OWASP

The Open Web Application Security Project



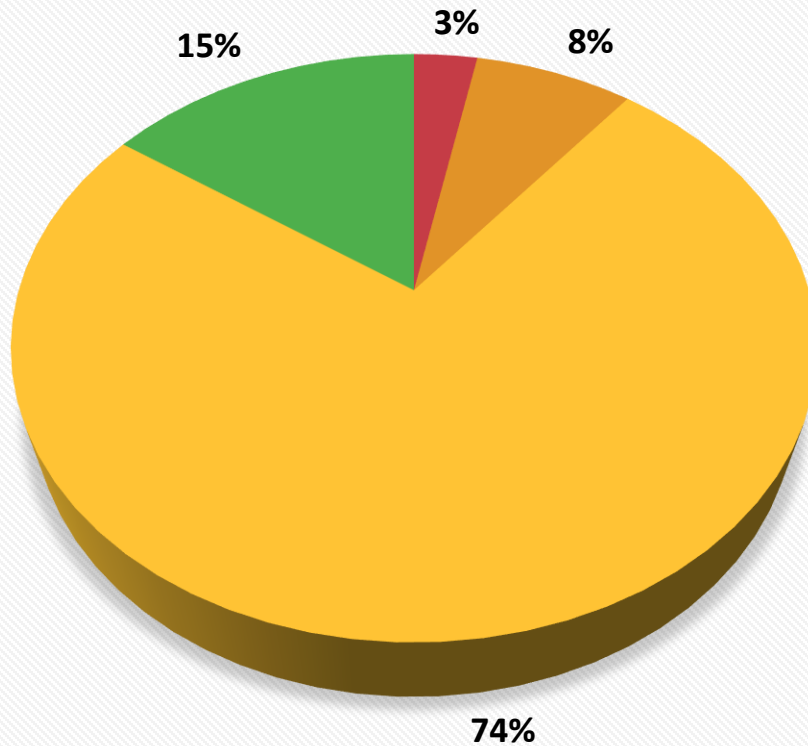


OWASP
The Open Web Application Security Project





Pregled ranjivosti po razinama



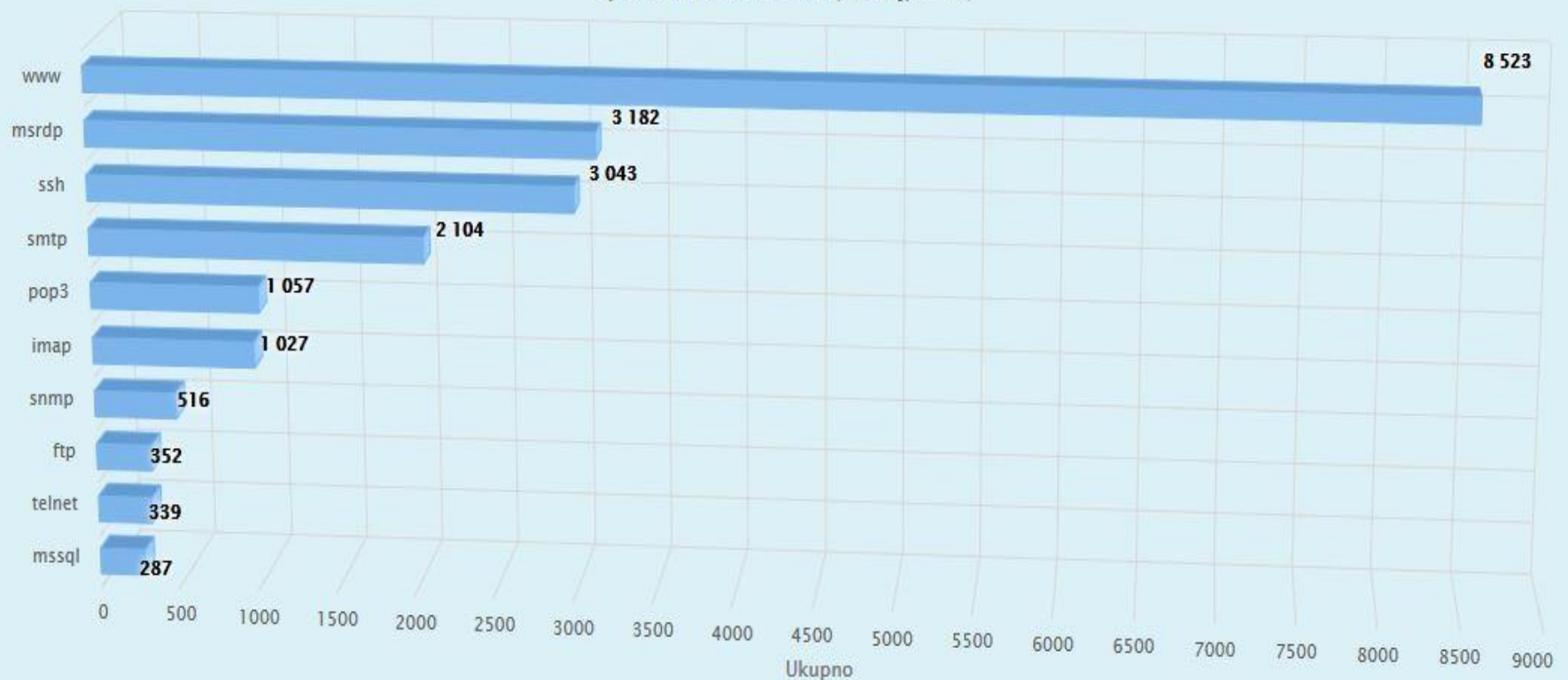
■ Kritične ■ Visoke ■ Srednje ■ Niske

Level	Number	Percentage
Kritične	706	3%
Visoke	1760	8%
Srednje	17007	74%
Niske	3509	15%
Total	22982	100%



Pregled ranjivih servisa

Tip ustanove: Sve ustanove (Travanj, 2016.)



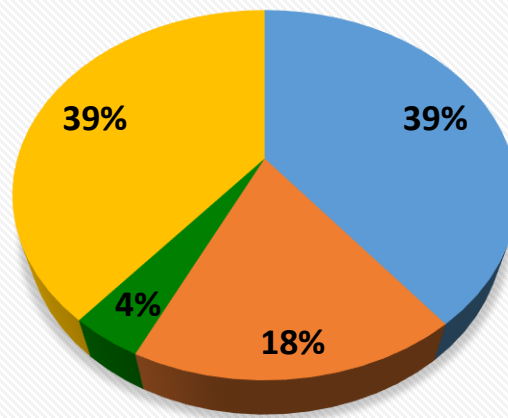


OWASP

The Open Web Application Security Project

- 5456 javno dostupnih adresa
- 1817 detektirano kao web server
 - 716 Apache
 - 321 Microsoft-IIS (5.0 - 10)
 - 71 nginx

Distribucija web servera



■ Apache ■ Microsoft-IIS ■ nginx ■ ostalo



OWASP

The Open Web Application Security Project

- Ranjivosti **kritične** razine:
 - OS sa isteklom podrškom (Windows/Unix)
 - Nepodržani i zastarjeli programski paketi
- Ranjivosti **visoke** razine:
 - Ranjivi servisi i programski paketi (Apache, PHP, OpenSSL, RDP...)
 - msrdp Remote Code Execution



OWASP

The Open Web Application Security Project

- Ranjivosti **srednje** razine:
 - korišćenje SSL v2/v3 protokola
 - msrdp MITM ranjivosti
 - Problemi sa SSL certifikatima (self-signed/expired)
 - DNS server spoofed request amplification DDoS
- Ranjivosti **niske** razine:
 - Korišćenje slabih kriptografskih algoritama
 - Clear Text Authentication (FTP, SMTP, POP3)



OWASP

The Open Web Application Security Project

- Shellshock
- Logjam
- BEAST
- Heartbleed
- DROWN
- GHOST
- Bar Mitzvah
- POODLE
- FREAK





„The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts.”

- Eugene H. Spafford



OWASP

The Open Web Application Security Project

Hvala na pažnji!

