(Ne)Sigurnost hrvatskog Internet prostora

OWASP

The Open Web Application Security Project

O meni

OWASP
The Open Web Application Security Project

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

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK
Nacionalni CERT

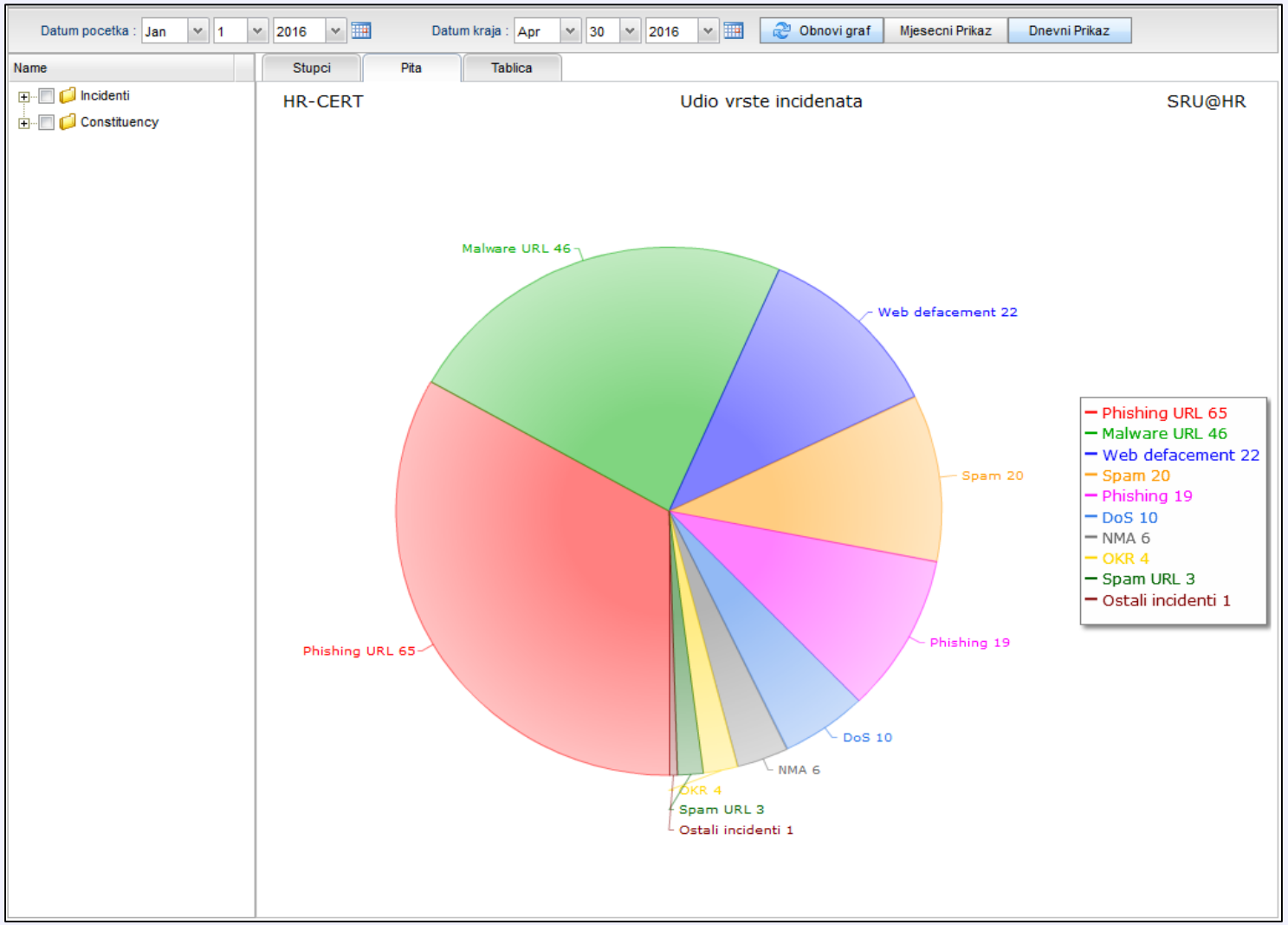
NCERT Do’s & Don’ts

OWASP
The Open Web Application Security Project

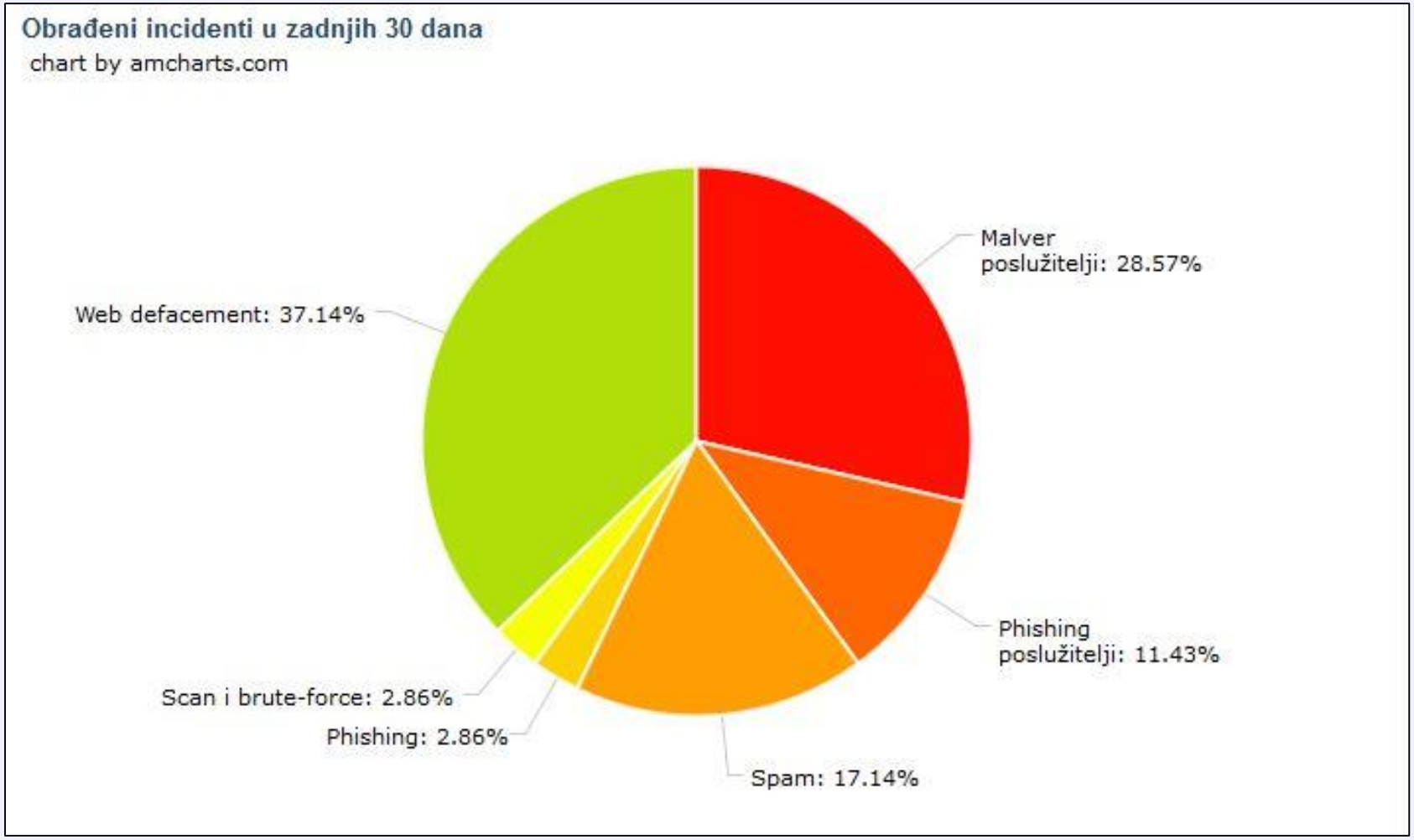
- ✓ Uklanjanje malicioznog sadržaja s Interneta
- ✓ Obrada incidenata na Internetu, ako se jedna od strana u incidentu nalazi u RH, osim tijela državne uprave (ZSIS CERT)
- ✓ Diseminacija informacija (vijesti, preporuke, dokumenti, brošure, alati)
- ✓ Forenzika, analiza malvera, mrežnog prometa, logova...

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

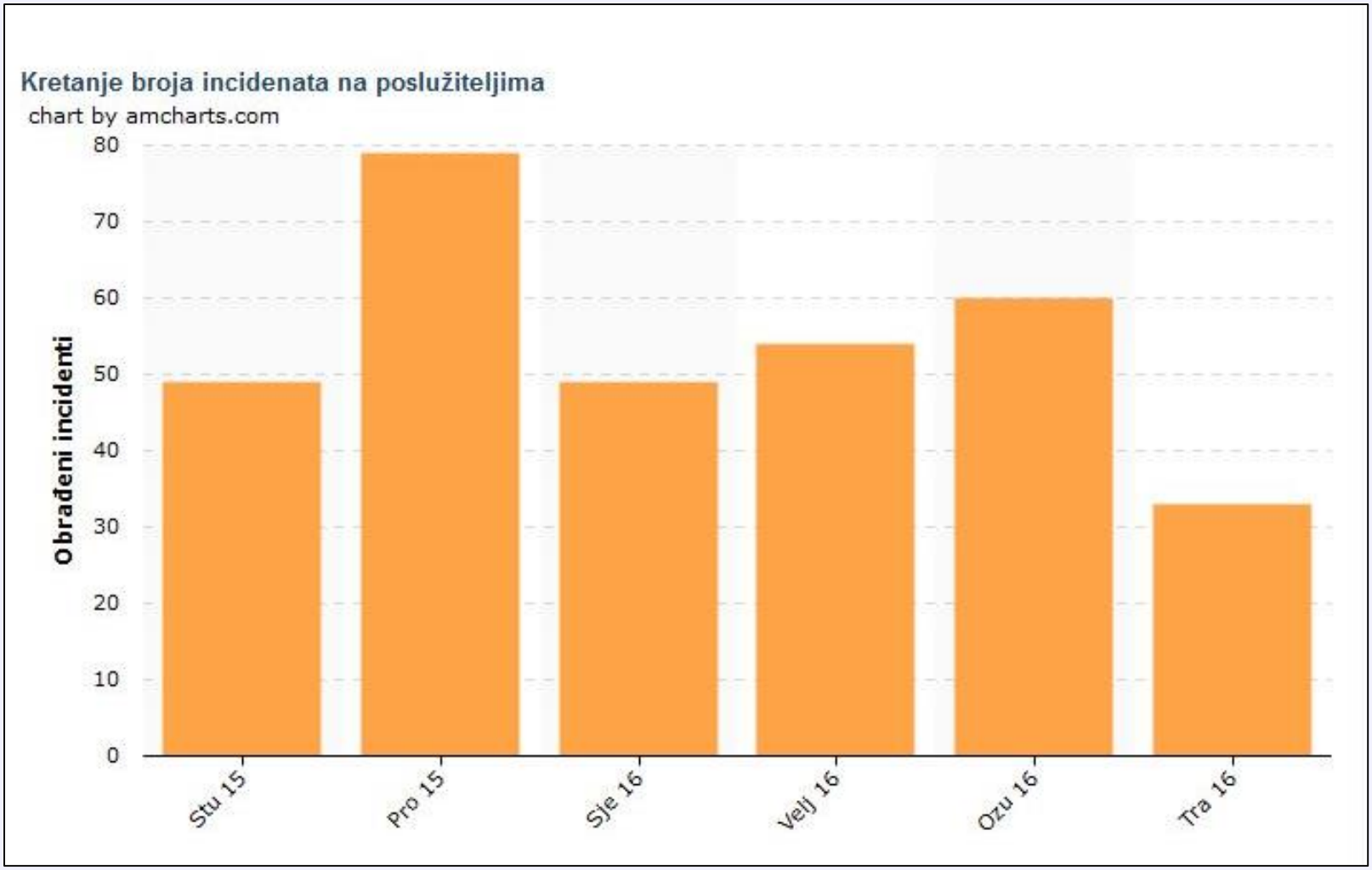
SRU@HR – vrste incidenata



OWASP
The Open Web Application Security Project

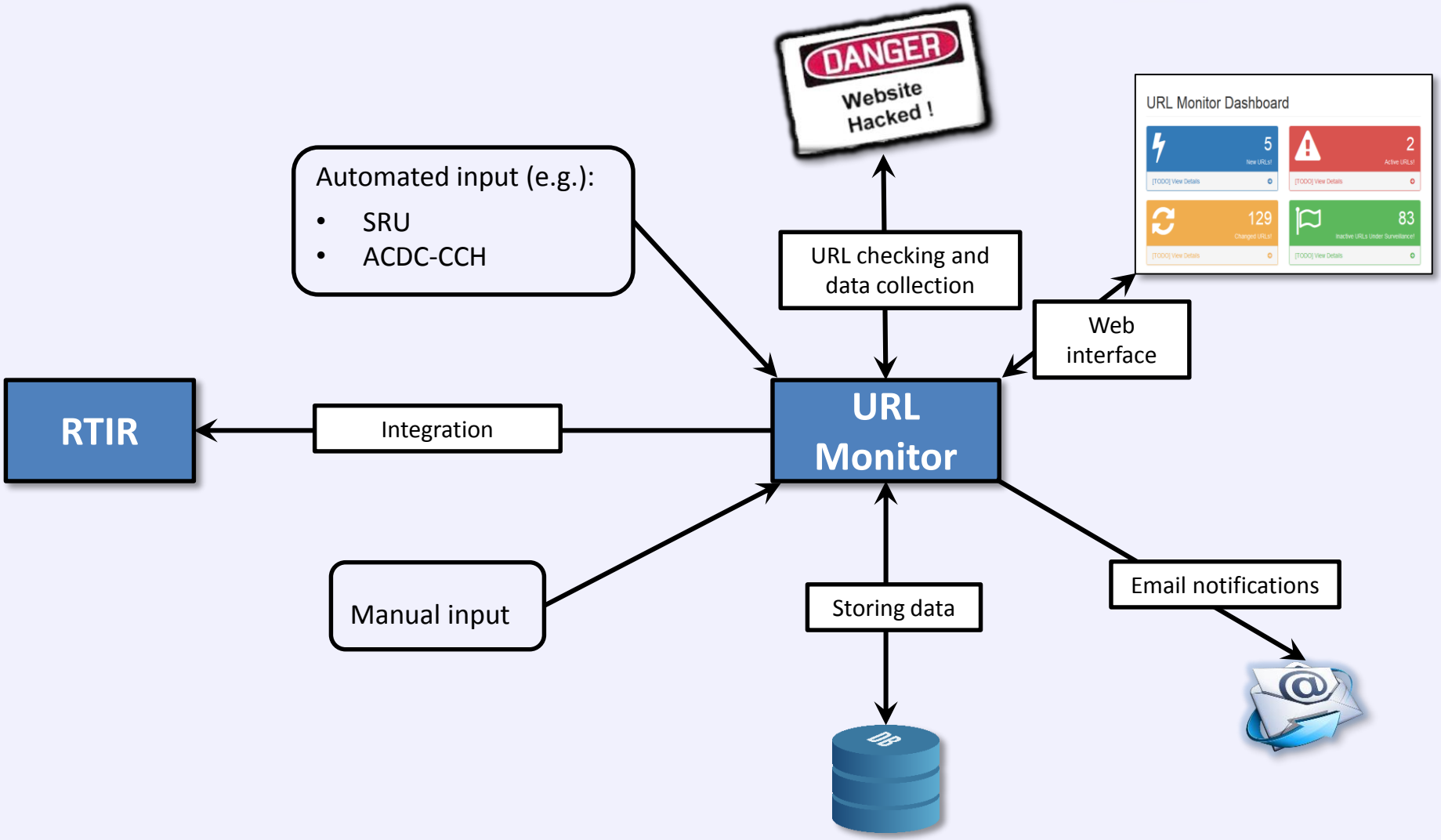


OWASP
The Open Web Application Security Project



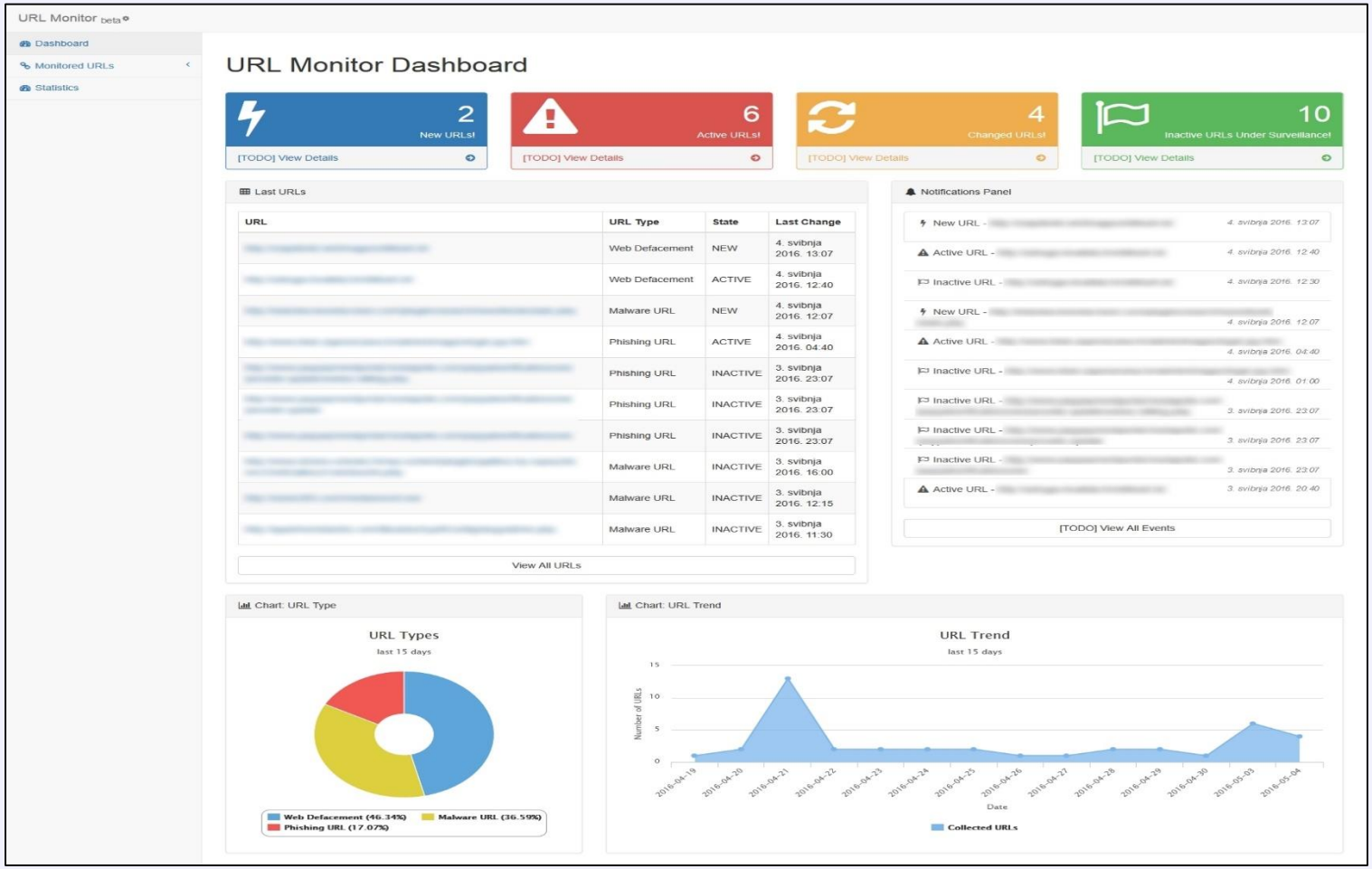
URL Monitor

OWASP
The Open Web Application Security Project



URL Monitor Dashboard

OWASP
The Open Web Application Security Project



URL details

URL Details

INACTIVE

URL:

IP Address:

URL Type:

Phishing URL

Domain:

Source:

SRU

DNS Data:

Frequency:

60

Redirect URL:

Country Code:

FR

Customer:

Monitor Type:

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	

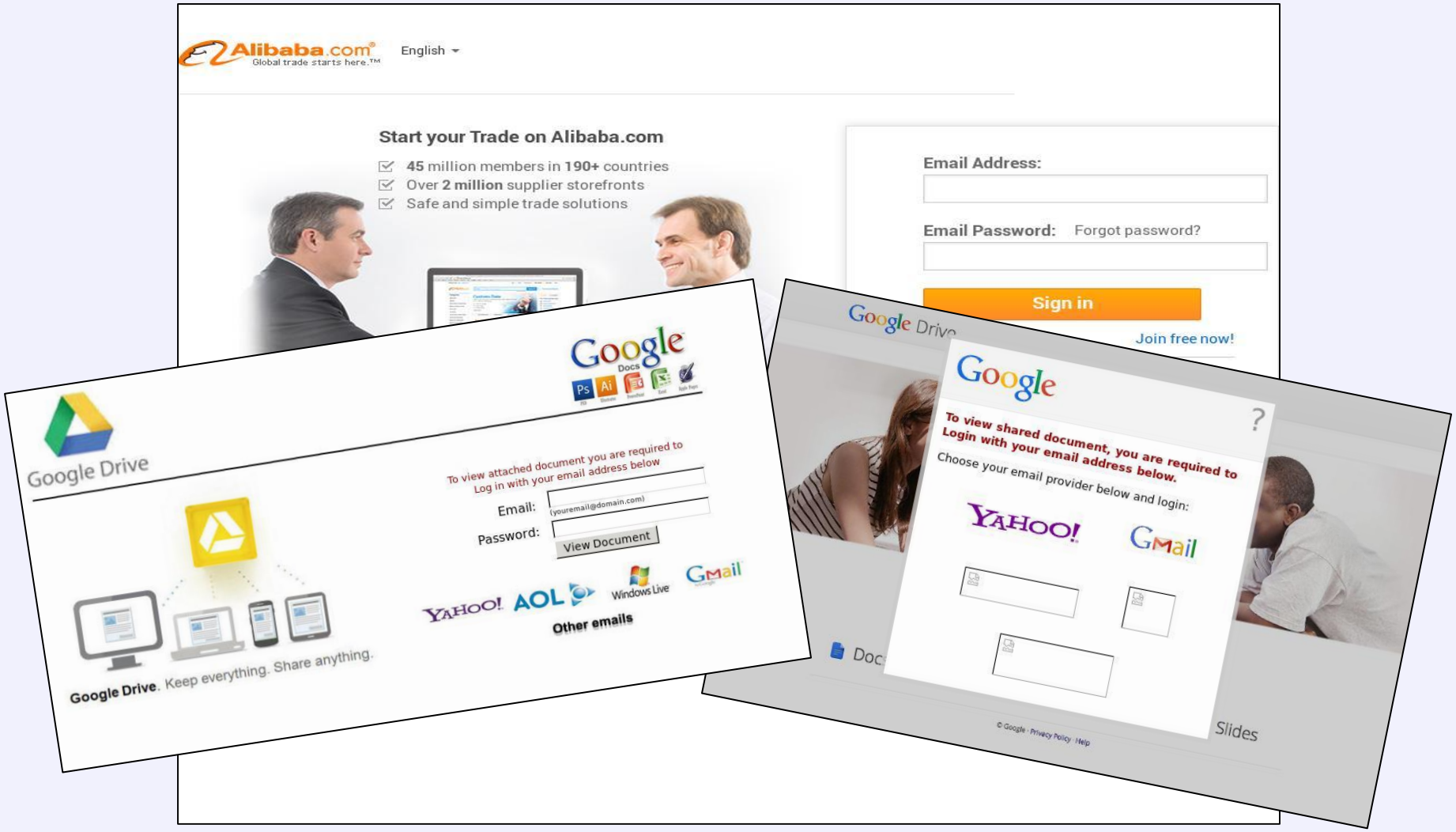
Showing 1 to 7 of 7 entries

‹ Previous 1 Next ›

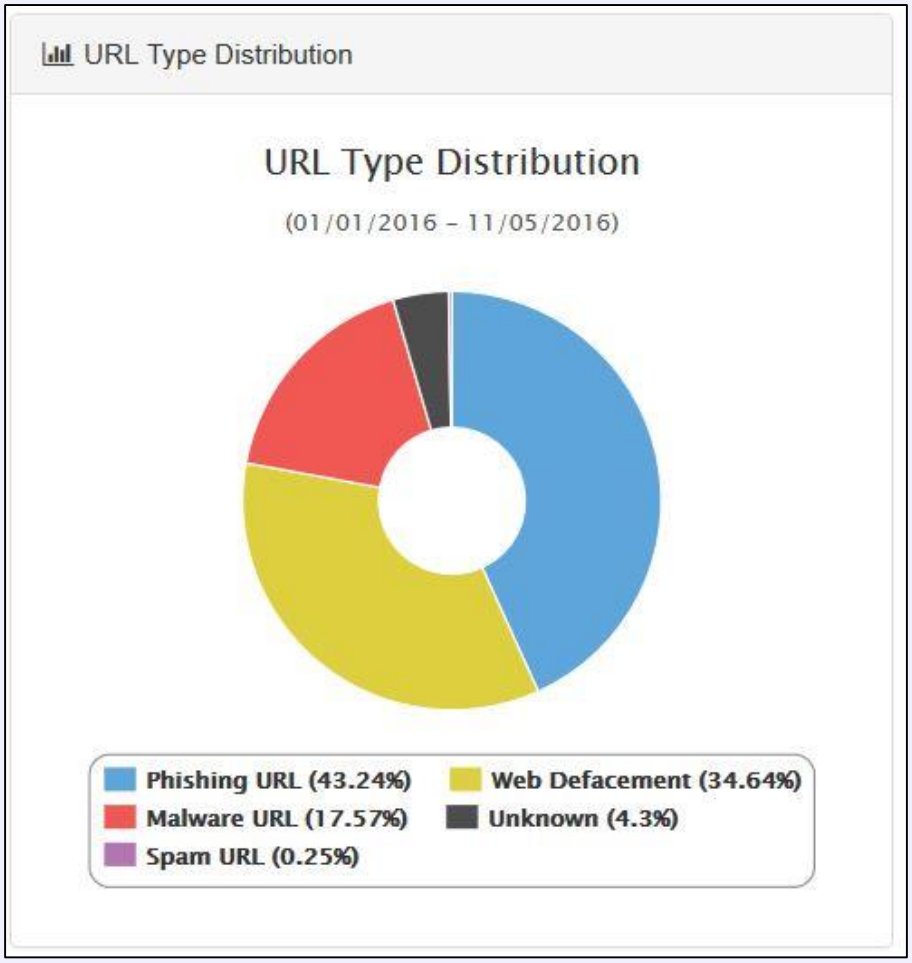
Web defacements

Phishing sites

OWASP
The Open Web Application Security Project

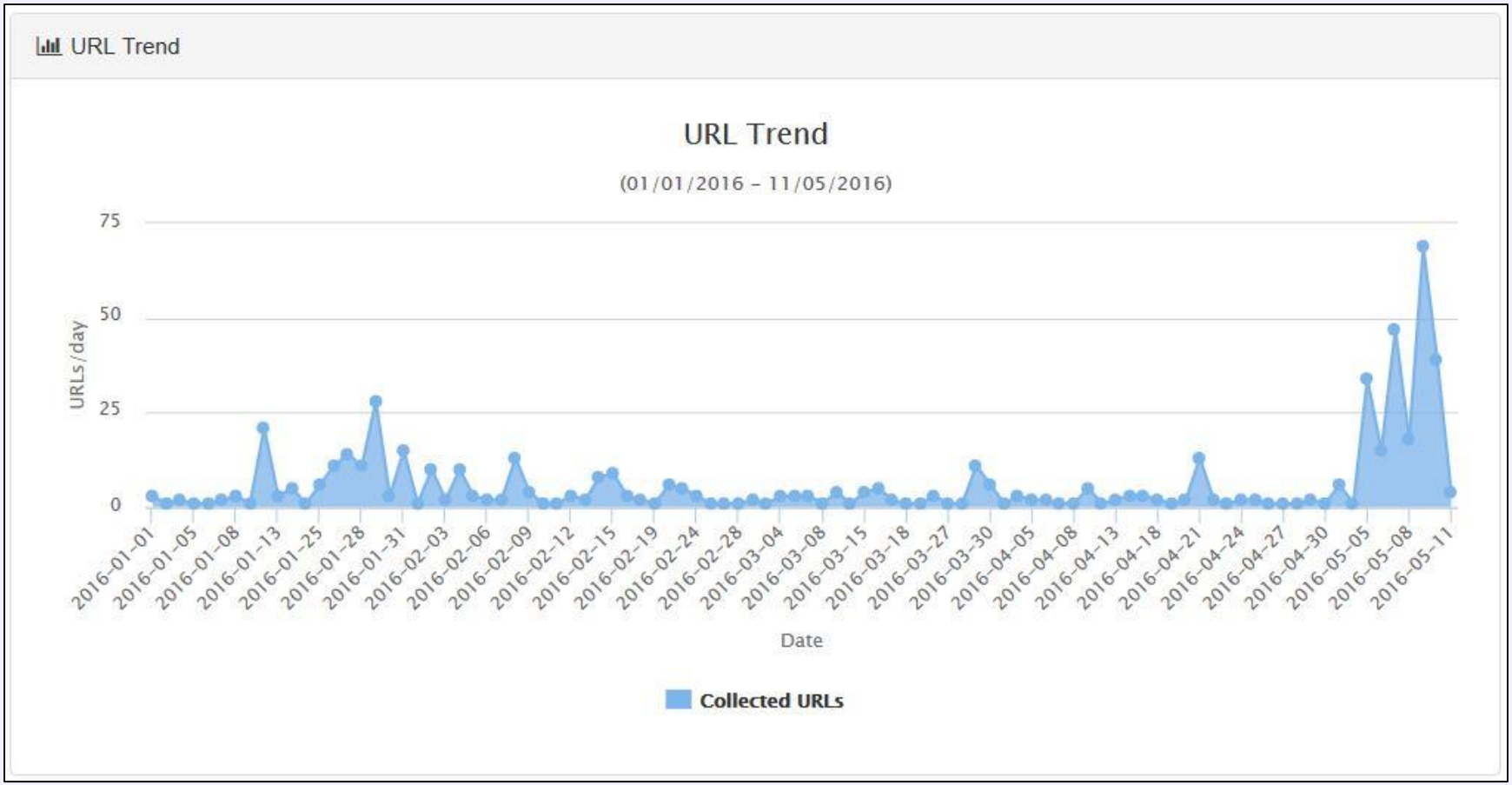


URL distribution



URL trend

OWASP
The Open Web Application Security Project



Obilježja akademskih/obrazovnih mreža

OWASP
The Open Web Application Security Project

- 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

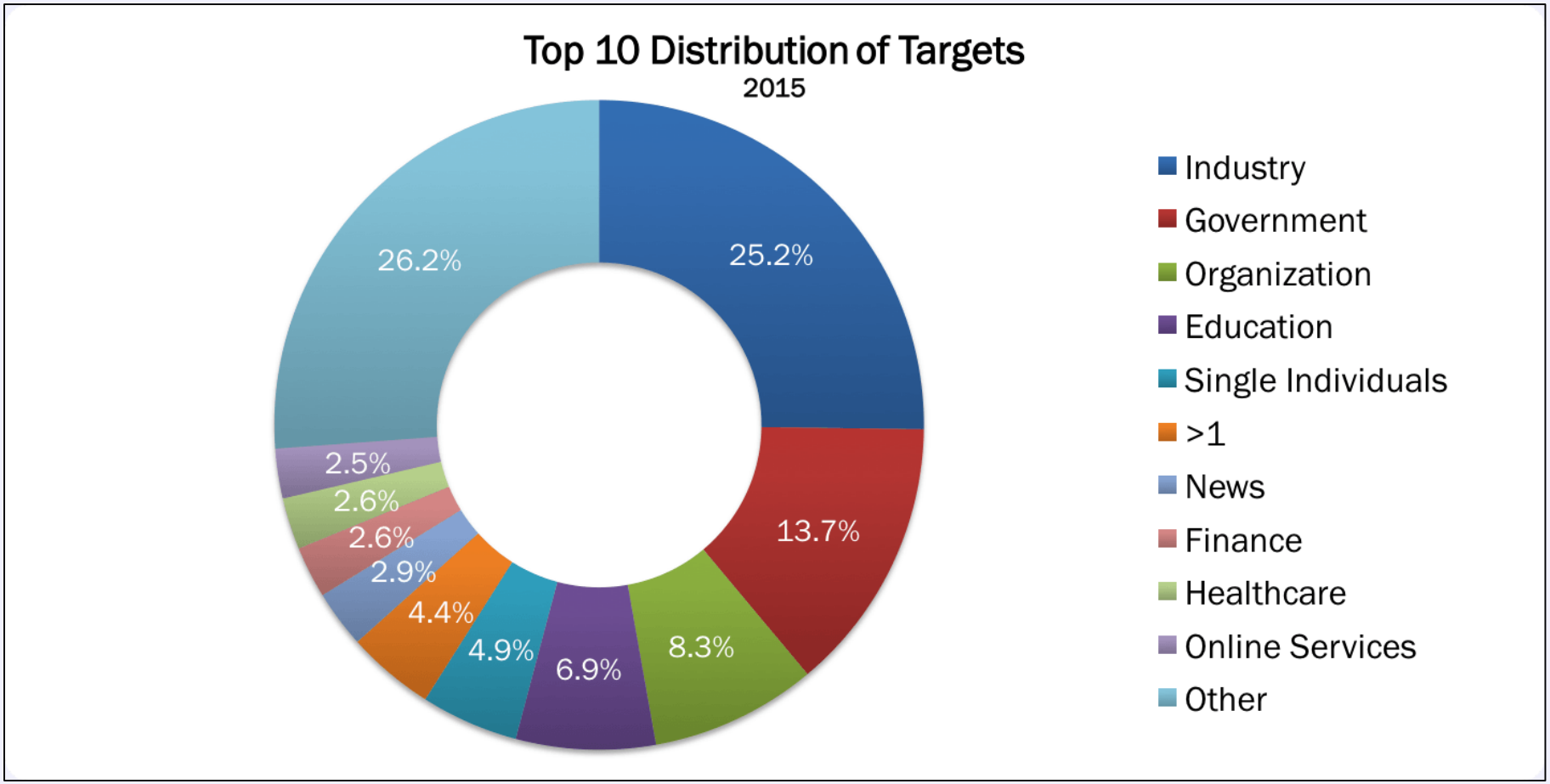
Napadi na akademske mreže

OWASP
The Open Web Application Security Project

- 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

Trendovi napada na internetu

OWASP
The Open Web Application Security Project

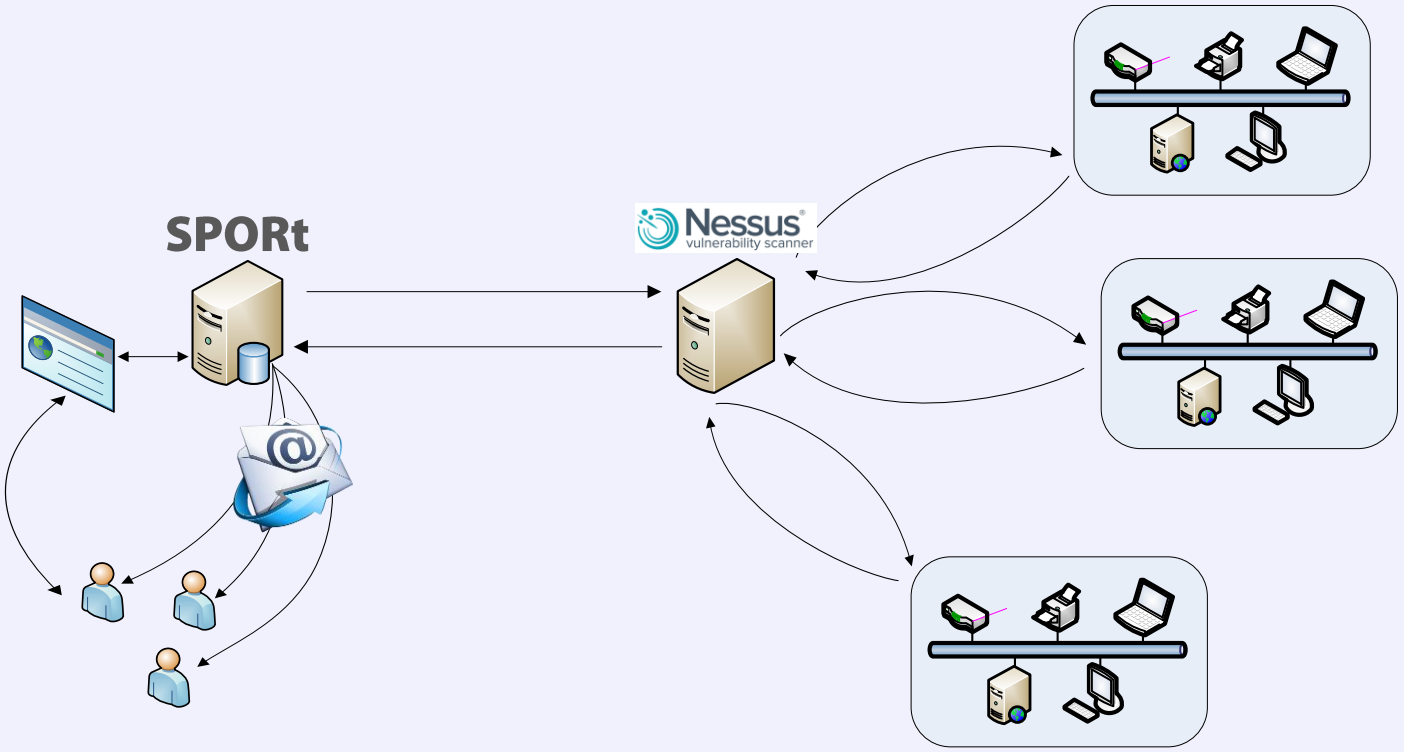


(Izvor: www.hackmageddon.com)

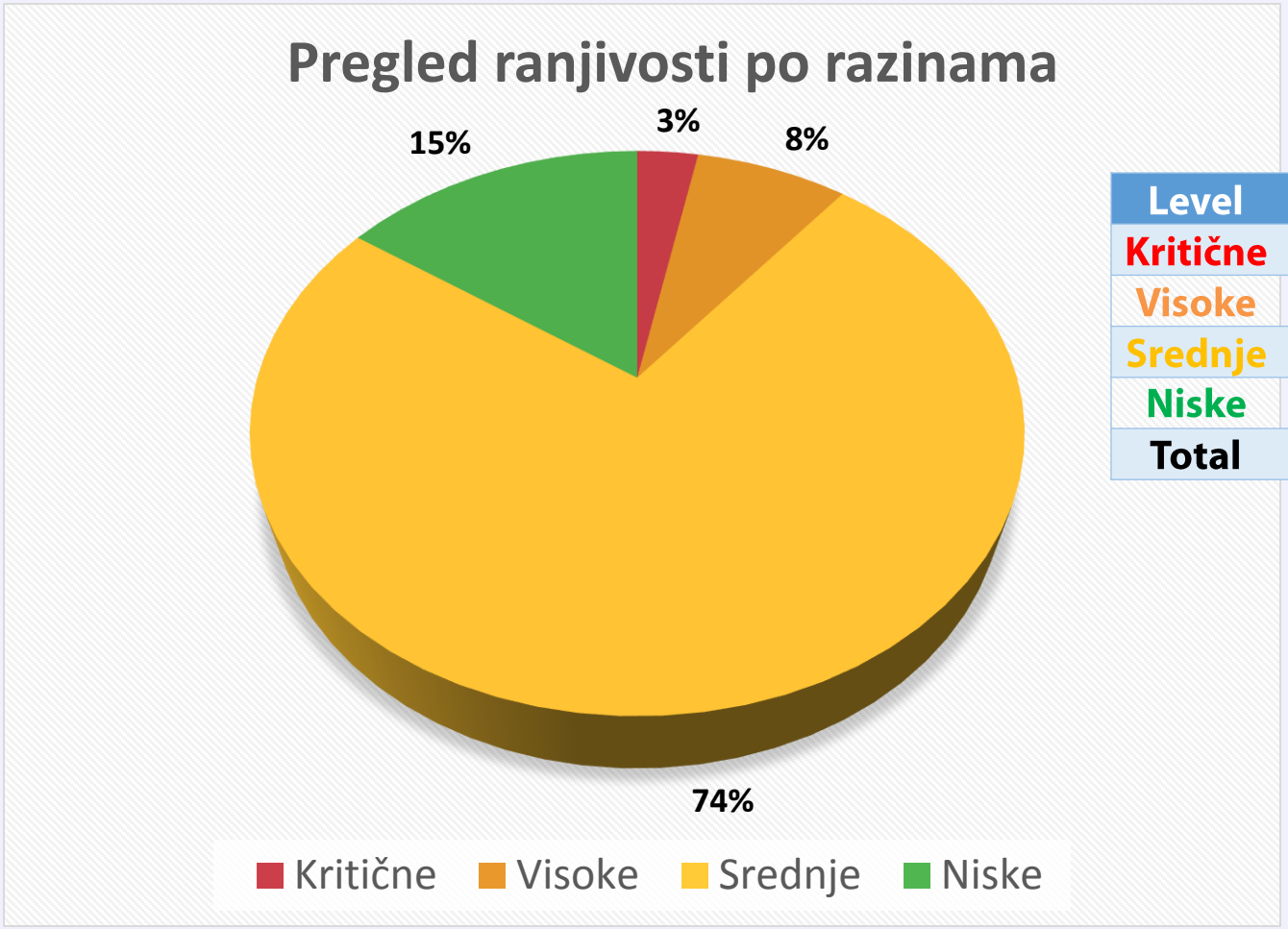
SPORt

OWASP
The Open Web Application Security Project

SPORt

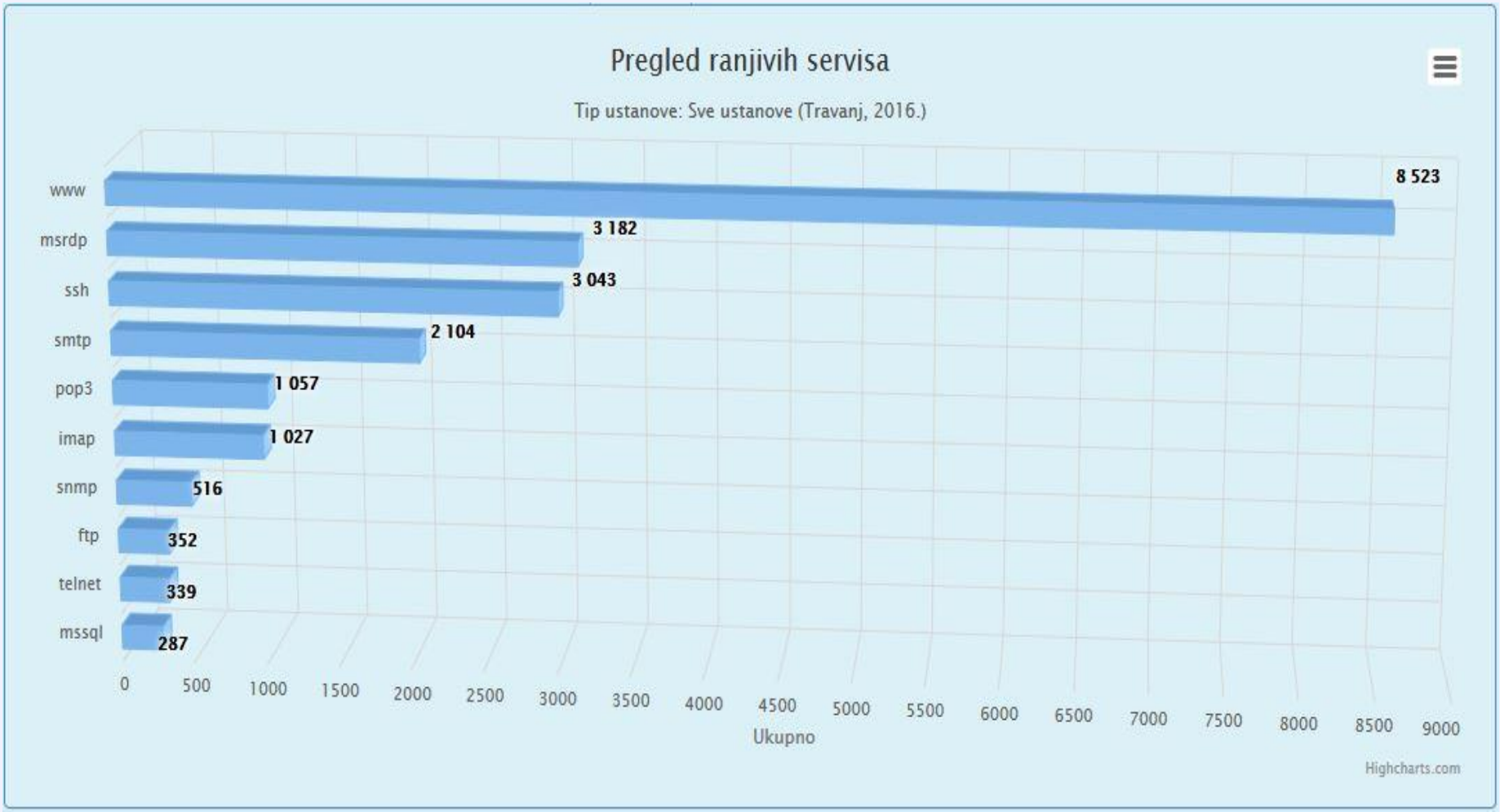


OWASP
The Open Web Application Security Project

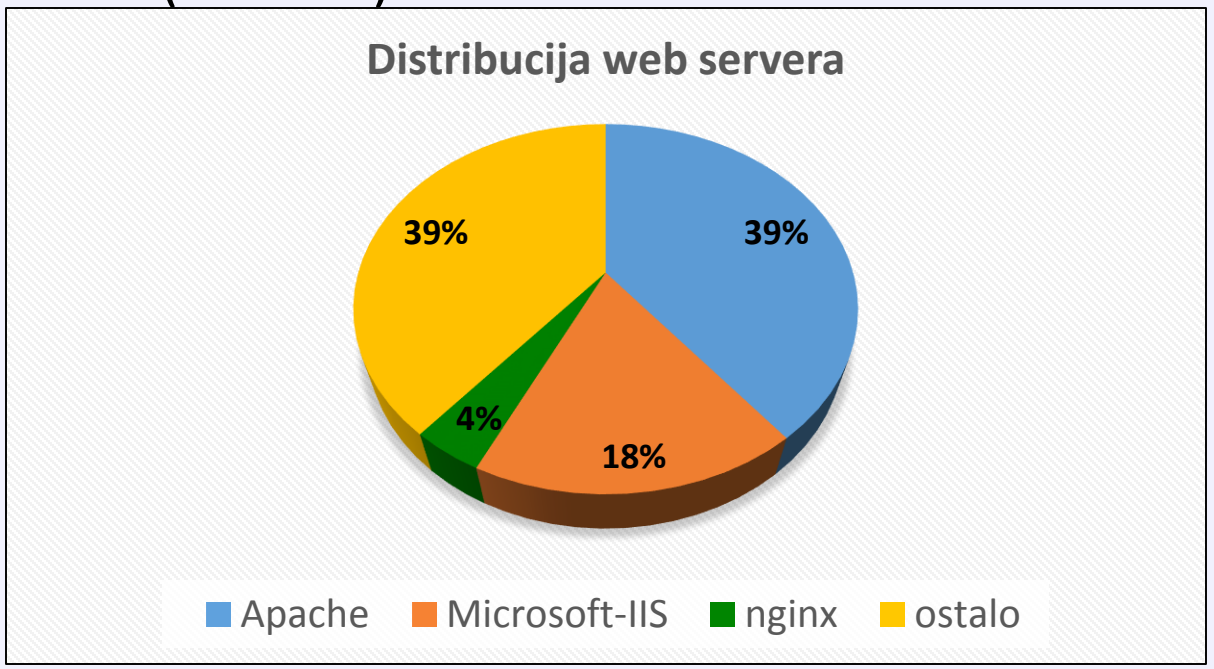


Level	Number	Percentage
Kritične	706	3%
Visoke	1760	8%
Srednje	17007	74%
Niske	3509	15%
Total	**22982**	100%

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



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

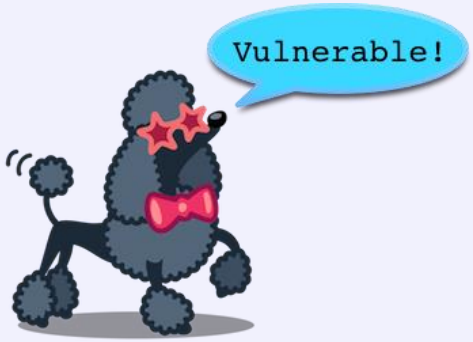
- Ranjivosti srednje razine:
  - korištenje SSL v2/v3 protokola
  - msrdp MITM ranjivosti
  - Problemi sa SSL certifikatima (self-signed/expired)
  - DNS server spoofed request amplification DDoS

- Ranjivosti niske razine:
  - Korištenje slabih kriptografskih algoritama
  - Clear Text Authentication (FTP, SMTP, POP3)

„Brand name” ranjivosti

OWASP
The Open Web Application Security Project

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



Umjesto zaključka

OWASP
The Open Web Application Security Project

„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

Hvala na pažnji!