Jornadas Computação Científica 2019

PORTUGAL INCoDe.2030

PyMonitor - GodZilla

Duarte Sousa

Centro Nacional de Cibersegurança

Patrocinadores **Platina**

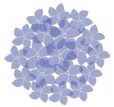
Patrocinadores **Ouro**

Patrocinadores **Prata**

Apoios

Organização

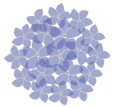
PyMonitor – GodZilla



- Melhoria constante dos processos de monitorização
- Âmbito da missão do Centro Nacional de Cibersegurança
  - Antecipar (incidentes ou ciberataques)
  - Detetar (incidentes ou ciberataques)
  - Reagir (a incidentes ou ciberataques)
  - Recuperar (de incidentes ou ciberataques)

- Criado em 2016 - PyMonitor GodZilla
- Simples script que recolhia os valores de carregamentos de um grupo predefinido de URLs.

PyMonitor – GodZilla: Bots



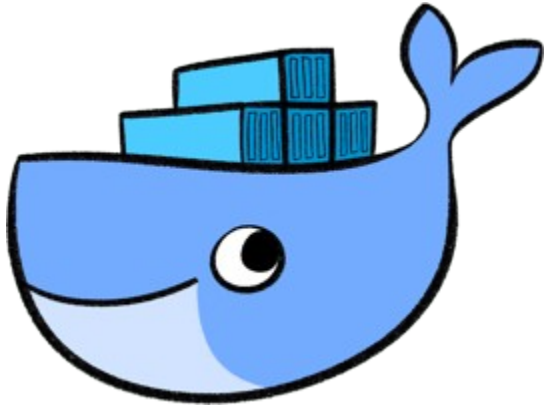
- Software modular,
- Objetivo:
  - Monitorização de um determinado site
  - Registando numa base de dados os valores recolhidos

- Atualmente conta com sete bots totalmente autónomos:
  - Bot LoadURL
  - Bot Deface
  - Bot JavaScript
  - Bot WordList
  - Bot Ping (icmp)
  - Bot DNS (Name Servers)
  - Bot CertificadosSSL

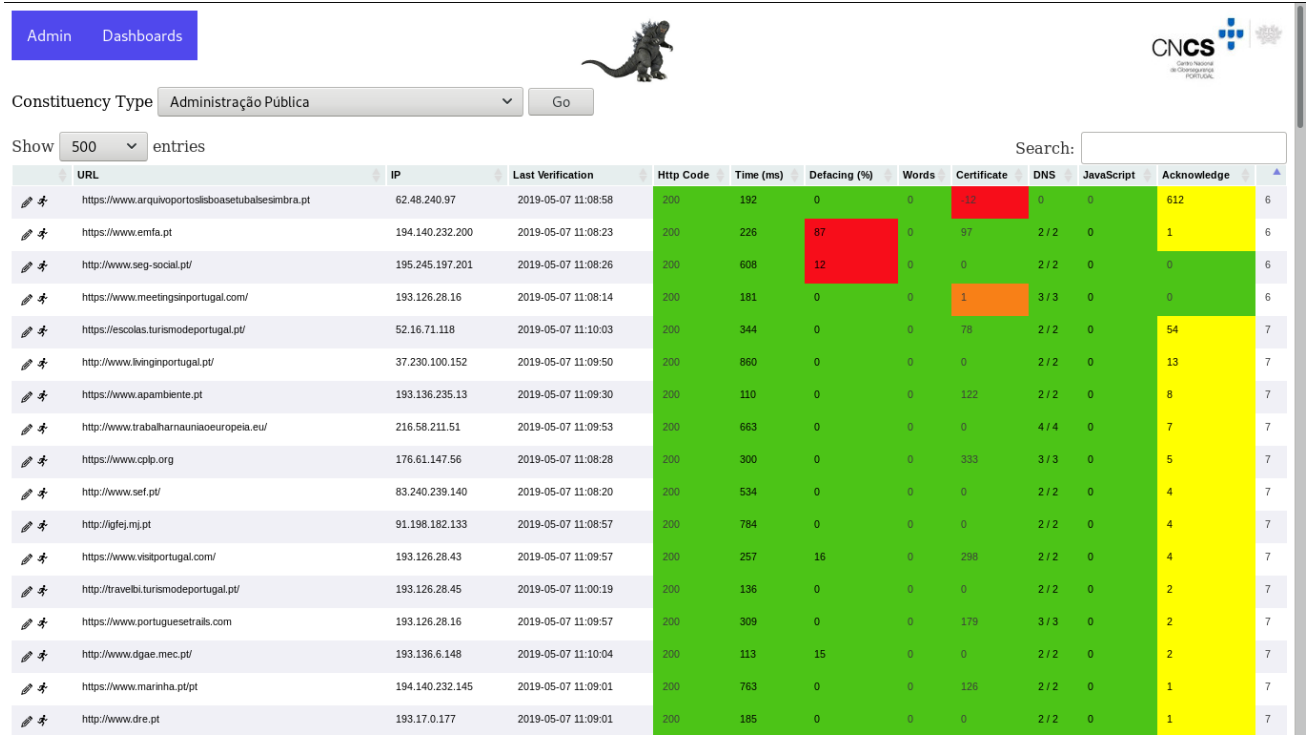
PyMonitor – GodZilla: Tecnologias usadas

python™

mongoDB.



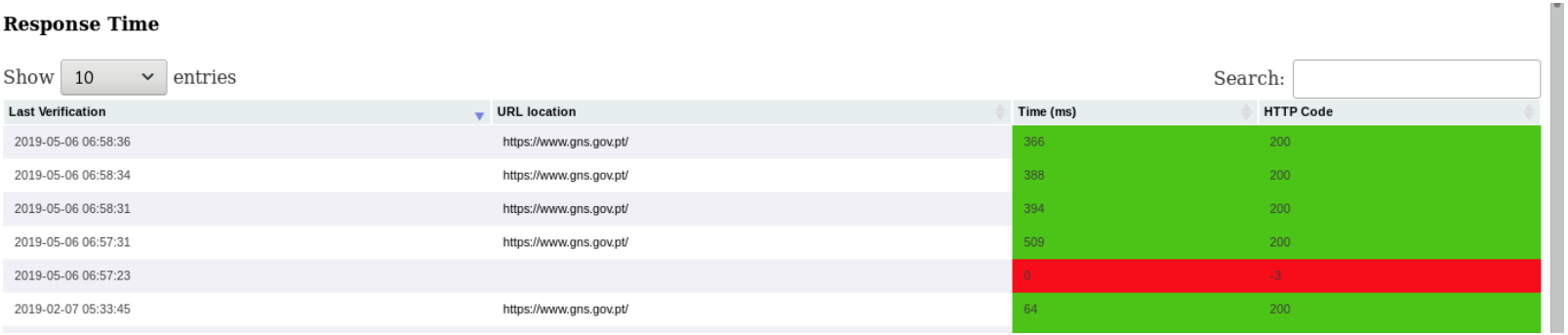
PyMonitor – GodZilla: Dashboard Principal



	URL	IP	Last Verification	Http Code	Time (ms)	Defacing (%)	Words	Certificate	DNS	JavaScript	Acknowledge	
	https://www.arquivoportoslisboasetubalsesimbra.pt	62.48.240.97	2019-05-07 11:08:58	200	192	0	0	-12	0	0	612	6
	https://www.emfa.pt	194.140.232.200	2019-05-07 11:08:23	200	226	87	0	97	2 / 2	0	1	6
	http://www.seg-social.pt/	195.245.197.201	2019-05-07 11:08:26	200	608	12	0	0	2 / 2	0	0	6
	https://www.meetingsinportugal.com/	193.126.28.16	2019-05-07 11:08:14	200	181	0	0	1	3 / 3	0	0	6
	https://escolas.turismodeportugal.pt/	52.16.71.118	2019-05-07 11:10:03	200	344	0	0	78	2 / 2	0	54	7
	http://www.livinginportugal.pt/	37.230.100.152	2019-05-07 11:09:50	200	860	0	0	0	2 / 2	0	13	7
	https://www.apambiente.pt	193.136.235.13	2019-05-07 11:09:30	200	110	0	0	122	2 / 2	0	8	7
	http://www.trabalharnauniaoeuropeia.eu/	216.58.211.51	2019-05-07 11:09:53	200	663	0	0	0	4 / 4	0	7	7
	https://www.cplp.org	176.61.147.56	2019-05-07 11:08:28	200	300	0	0	333	3 / 3	0	5	7
	http://www.sef.pt/	83.240.239.140	2019-05-07 11:08:20	200	534	0	0	0	2 / 2	0	4	7
	http://igfej.mj.pt	91.198.182.133	2019-05-07 11:08:57	200	784	0	0	0	2 / 2	0	4	7
	https://www.visitportugal.com/	193.126.28.43	2019-05-07 11:09:57	200	257	16	0	298	2 / 2	0	4	7
	http://travelbi.turismodeportugal.pt/	193.126.28.45	2019-05-07 11:00:19	200	136	0	0	0	2 / 2	0	2	7
	https://www.portuguesetrails.com	193.126.28.16	2019-05-07 11:09:57	200	309	0	0	179	3 / 3	0	2	7
	http://www.dgae.mec.pt/	193.136.6.148	2019-05-07 11:10:04	200	113	15	0	0	2 / 2	0	2	7
	https://www.marinha.pt/pt	194.140.232.145	2019-05-07 11:09:01	200	763	0	0	126	2 / 2	0	1	7
	http://www.dre.pt	193.17.0.177	2019-05-07 11:09:01	200	185	0	0	0	2 / 2	0	1	7

PyMonitor – GodZilla: Bot LoadURL

- Recolhe valores de carregamentos de um site
- Recolhe código HTML da primeira página



Response Time

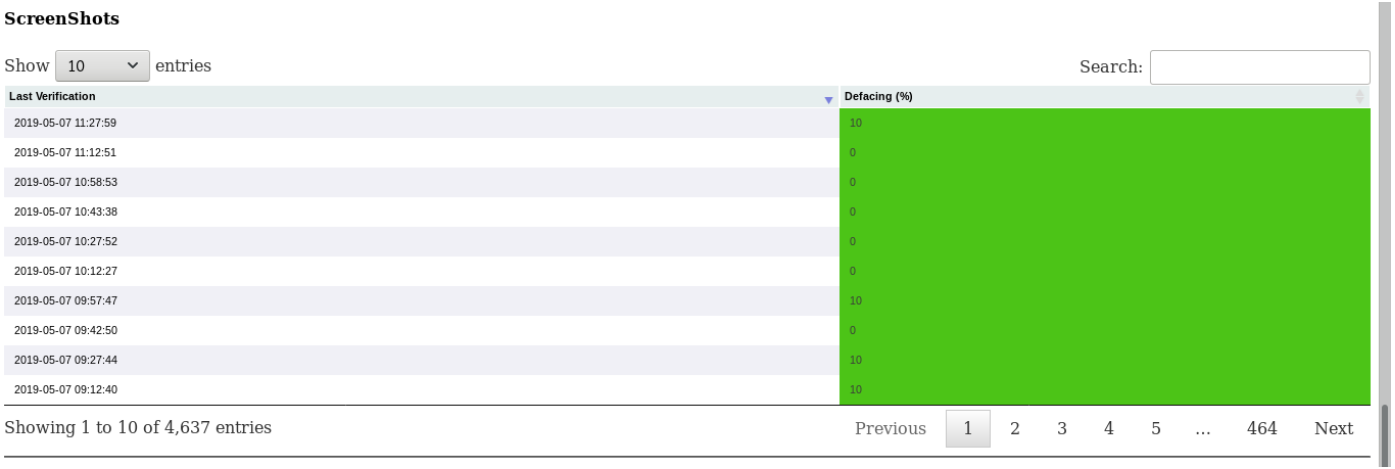
Show 10 entries

Search:

Last Verification	URL location	Time (ms)	HTTP Code
2019-05-06 06:58:36	https://www.gns.gov.pt/	366	200
2019-05-06 06:58:34	https://www.gns.gov.pt/	388	200
2019-05-06 06:58:31	https://www.gns.gov.pt/	394	200
2019-05-06 06:57:31	https://www.gns.gov.pt/	509	200
2019-05-06 06:57:23		0	-3
2019-02-07 05:33:45	https://www.gns.gov.pt/	64	200

PyMonitor – GodZilla: Bot Deface

- Faz um screenshot do site e compara com o último screenshot
- Comparação feita pixel a pixel entre os dois screenshots
- Retorna o valor da percentagem da diferença



ScreenShots

Show 10 entries

Search:

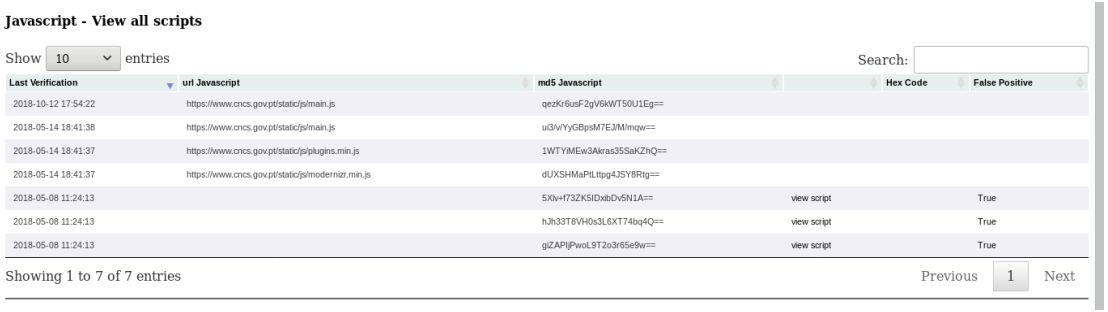
Last Verification	Defacing (%)
2019-05-07 11:27:59	10
2019-05-07 11:12:51	0
2019-05-07 10:58:53	0
2019-05-07 10:43:38	0
2019-05-07 10:27:52	0
2019-05-07 10:12:27	0
2019-05-07 09:57:47	10
2019-05-07 09:42:50	0
2019-05-07 09:27:44	10
2019-05-07 09:12:40	10

Showing 1 to 10 of 4,637 entries

Previous 1 2 3 4 5 … 464 Next

PyMonitor – GodZilla: Bot JavaScript

- Recebe o código HTML de um site e faz *parse* de todas as tags Javascript:
- Ficheiros javascript (*.js):
  - Download do script
  - Calcula hash MD5
  - Valida se a hash existe na base de dados, caso não exista, guarda
- Tags JavaScript:
  - Calculada a hash MD5 com base na string
  - Valida se a hash existe na base de dados, caso não exista, guarda



Javascript - View all scripts

Show 10 entries Search:

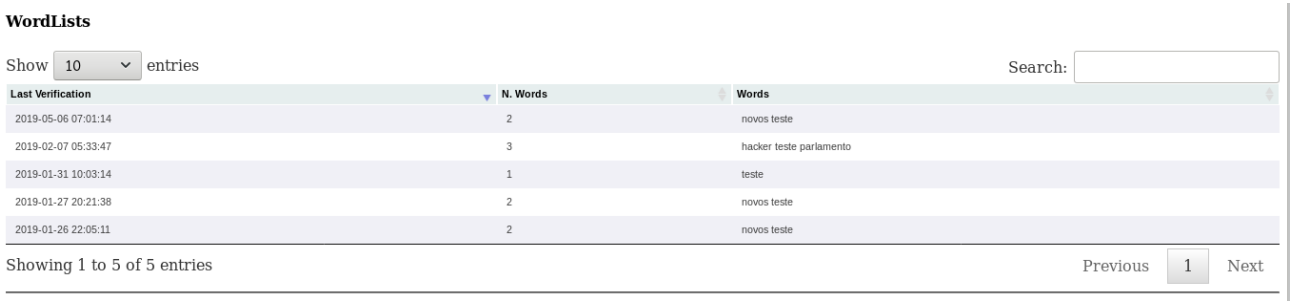
Last Verification	url Javascript	md5 Javascript		Hex Code	False Positive
2018-10-12 17:54:22	https://www.cncs.gov.pt/static/js/main.js	qezKr6usF2gV6kWT50U1Eg==			
2018-05-14 18:41:38	https://www.cncs.gov.pt/static/js/main.js	ui3/vlYyGBpsM7EJ/M/mqw==			
2018-05-14 18:41:37	https://www.cncs.gov.pt/static/js/plugins.min.js	1WTYiMEw3Akras35SaKZhQ==			
2018-05-14 18:41:37	https://www.cncs.gov.pt/static/js/modernizr.min.js	dUXSHMaPtLttpg4JSY8Rtg==			
2018-05-08 11:24:13		5Xlv+f73ZK5IDxibDv5N1A==	view script		True
2018-05-08 11:24:13		hJh33T8VH0s3L6XT74bq4Q==	view script		True
2018-05-08 11:24:13		giZAPIjPwoL9T2o3r65e9w==	view script		True

Showing 1 to 7 of 7 entries Previous 1 Next

PyMonitor – GodZilla: Bot WordLists

- É alimentado por *wordlists*
- Procura as palavras no código HTML

- Exemplos:
  - “Hacked By”
  - “Anonymous”
  - “Coinhive”
  - …



WordLists

Show 10 entries Search:

Last Verification	N. Words	Words
2019-05-06 07:01:14	2	novos teste
2019-02-07 05:33:47	3	hacker teste parlamento
2019-01-31 10:03:14	1	teste
2019-01-27 20:21:38	2	novos teste
2019-01-26 22:05:11	2	novos teste

Showing 1 to 5 of 5 entries Previous 1 Next

PyMonitor – GodZilla: Bot Ping (ICMP)

- Testa a disponibilidade do servidor através de Pings em períodos constantes

PyMonitor – GodZilla: Bot DNS (Name Servers)

- Valida quais são os *Name Servers* disponíveis na zona
- Valida a sua disponibilidade

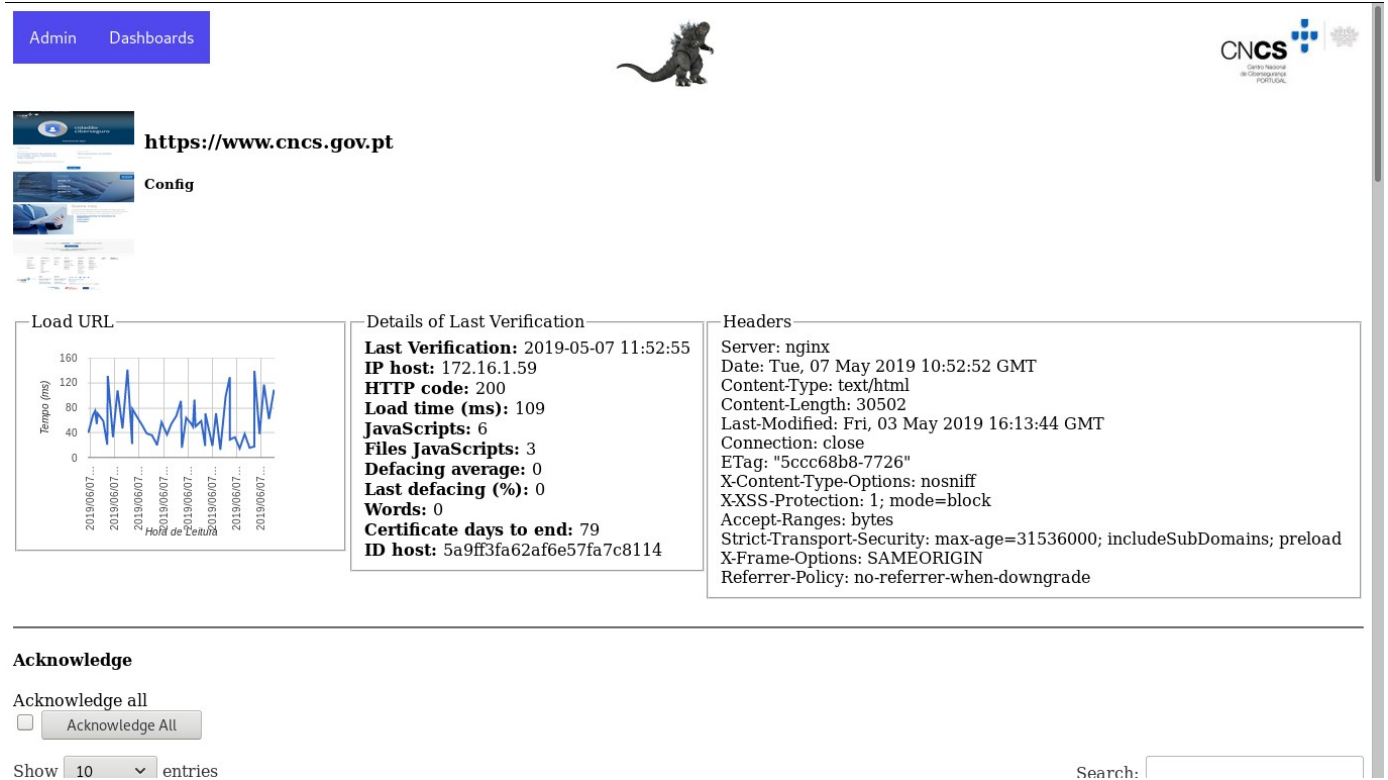
DNS

Zone: sapo.pt.
Last Validation: 2019-05-06 07:01:30
Total NS: 4
NS Online: ns.sapo.pt ns2.sapo.pt dns01.sapo.pt dns02.sapo.pt
NS Offline:

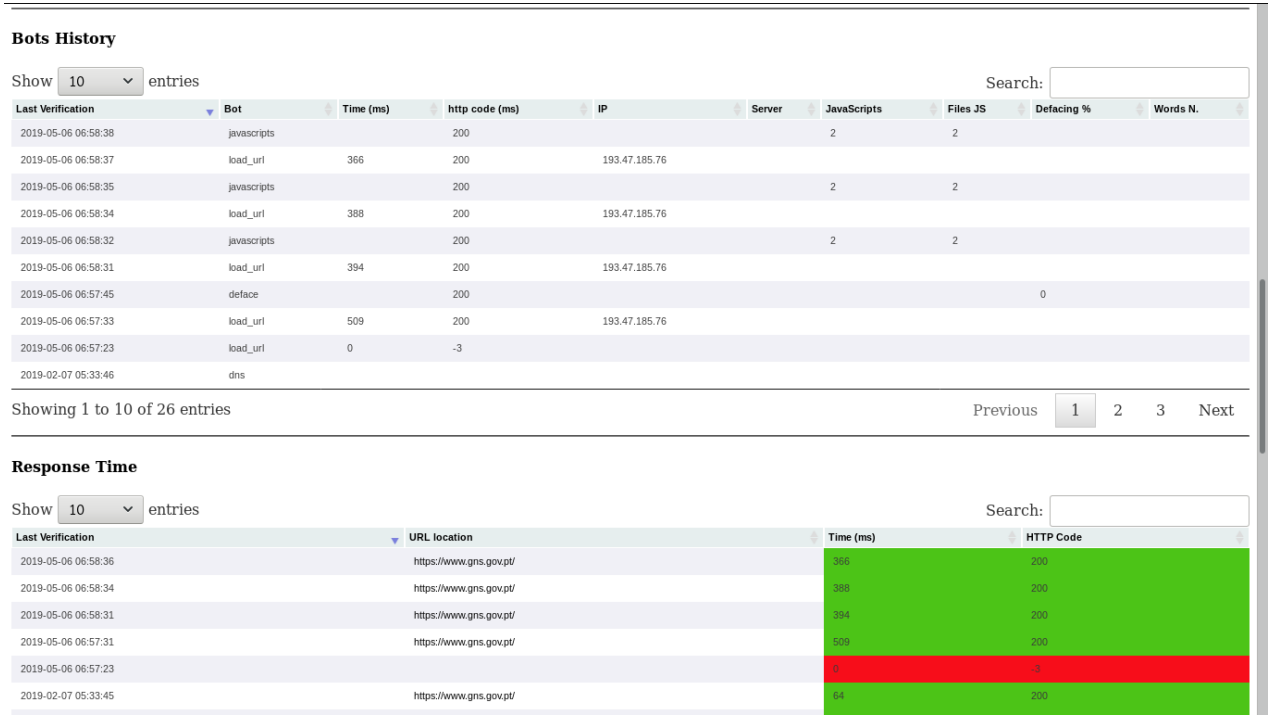
PyMonitor – GodZilla: Bot Certificados SSL

- Valida o certificado de um site
- Verifica a data de experição de forma a notificar a entidade com antecedência

PyMonitor – GodZilla: Site/Host Detalhes 1/3



PyMonitor – GodZilla: Site/Host Detalhes 2/3



Bots History

Show 10 entries Search:

Last Verification	Bot	Time (ms)	http code (ms)	IP	Server	JavaScripts	Files JS	Defacing %	Words N.
2019-05-06 06:58:38	javascripts		200			2	2		
2019-05-06 06:58:37	load_url	366	200	193.47.185.76					
2019-05-06 06:58:35	javascripts		200			2	2		
2019-05-06 06:58:34	load_url	388	200	193.47.185.76					
2019-05-06 06:58:32	javascripts		200			2	2		
2019-05-06 06:58:31	load_url	394	200	193.47.185.76					
2019-05-06 06:57:45	deface		200					0	
2019-05-06 06:57:33	load_url	509	200	193.47.185.76					
2019-05-06 06:57:23	load_url	0	-3						
2019-02-07 05:33:46	dns								

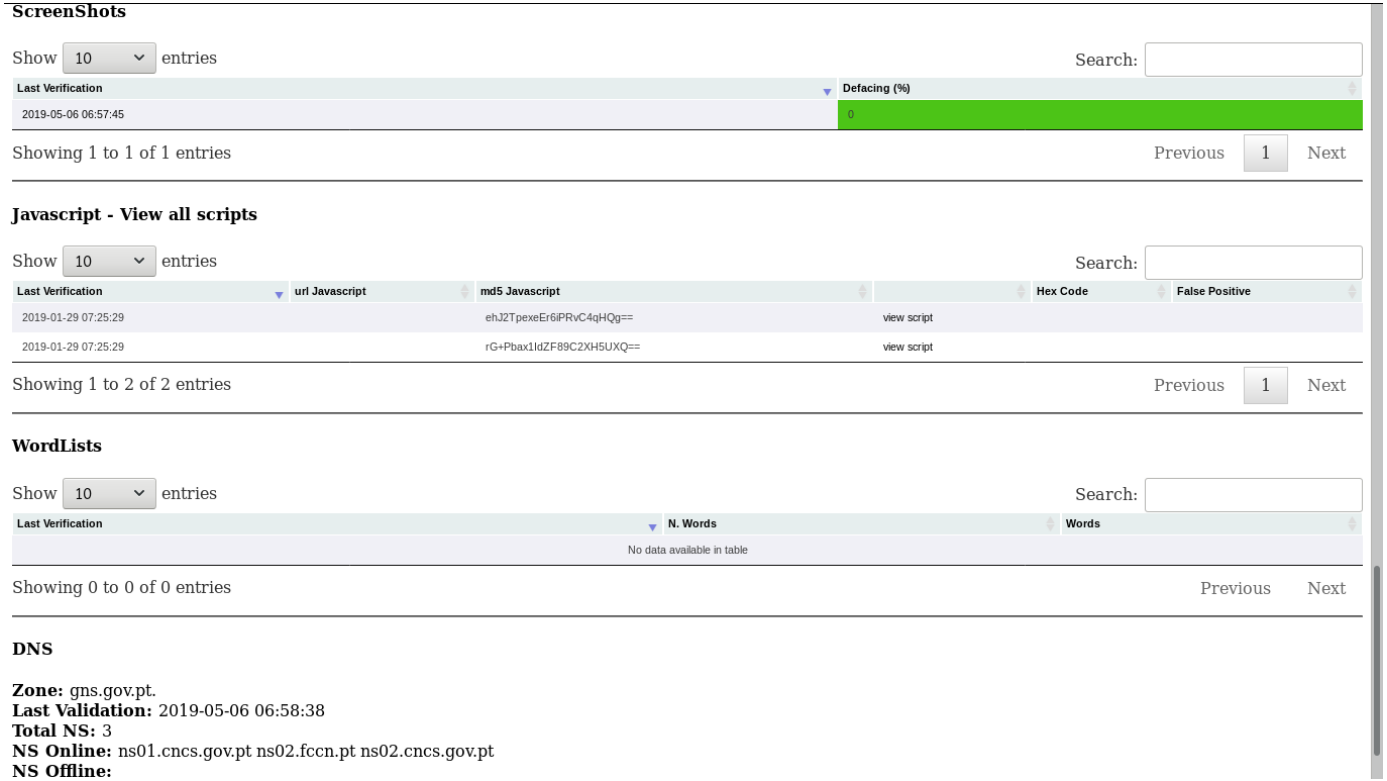
Showing 1 to 10 of 26 entries Previous 1 2 3 Next

Response Time

Show 10 entries Search:

Last Verification	URL location	Time (ms)	HTTP Code
2019-05-06 06:58:36	https://www.gns.gov.pt/	366	200
2019-05-06 06:58:34	https://www.gns.gov.pt/	388	200
2019-05-06 06:58:31	https://www.gns.gov.pt/	394	200
2019-05-06 06:57:31	https://www.gns.gov.pt/	509	200
2019-05-06 06:57:23		0	-3
2019-02-07 05:33:45	https://www.gns.gov.pt/	64	200

PyMonitor – GodZilla: Site/Host Detalhes 3/3



ScreenShots

Show 10 entries Search:

Last Verification	Defacing (%)
2019-05-06 06:57:45	0

Showing 1 to 1 of 1 entries Previous 1 Next

Javascript - View all scripts

Show 10 entries Search:

Last Verification	url Javascript	md5 Javascript		Hex Code	False Positive
2019-01-29 07:25:29		ehJ2TpexeEr6iPRvC4qHQg==	view script		
2019-01-29 07:25:29		rG+Pbax1ldZF89C2XH5UXQ==	view script		

Showing 1 to 2 of 2 entries Previous 1 Next

WordLists

Show 10 entries Search:

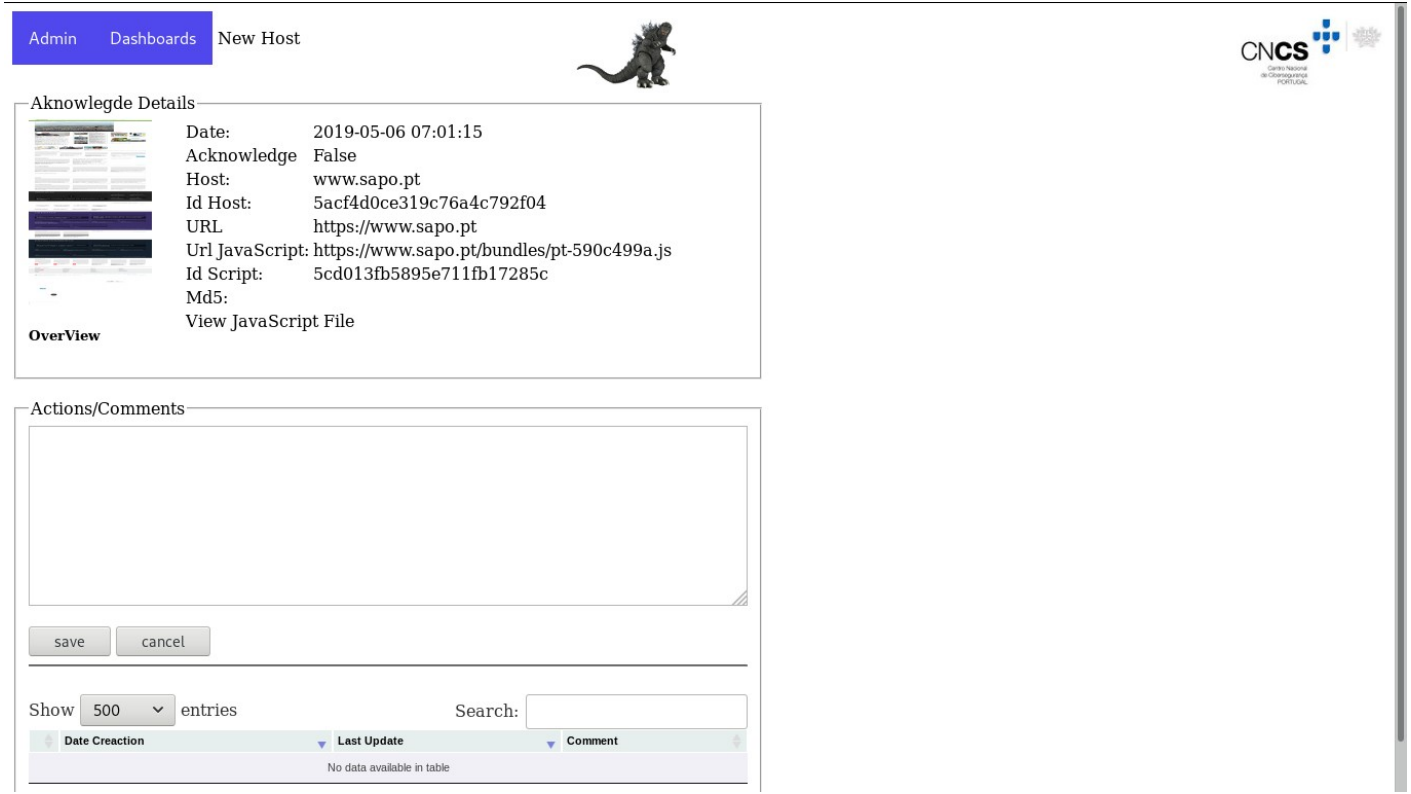
Last Verification	N. Words	Words
No data available in table		

Showing 0 to 0 of 0 entries Previous Next

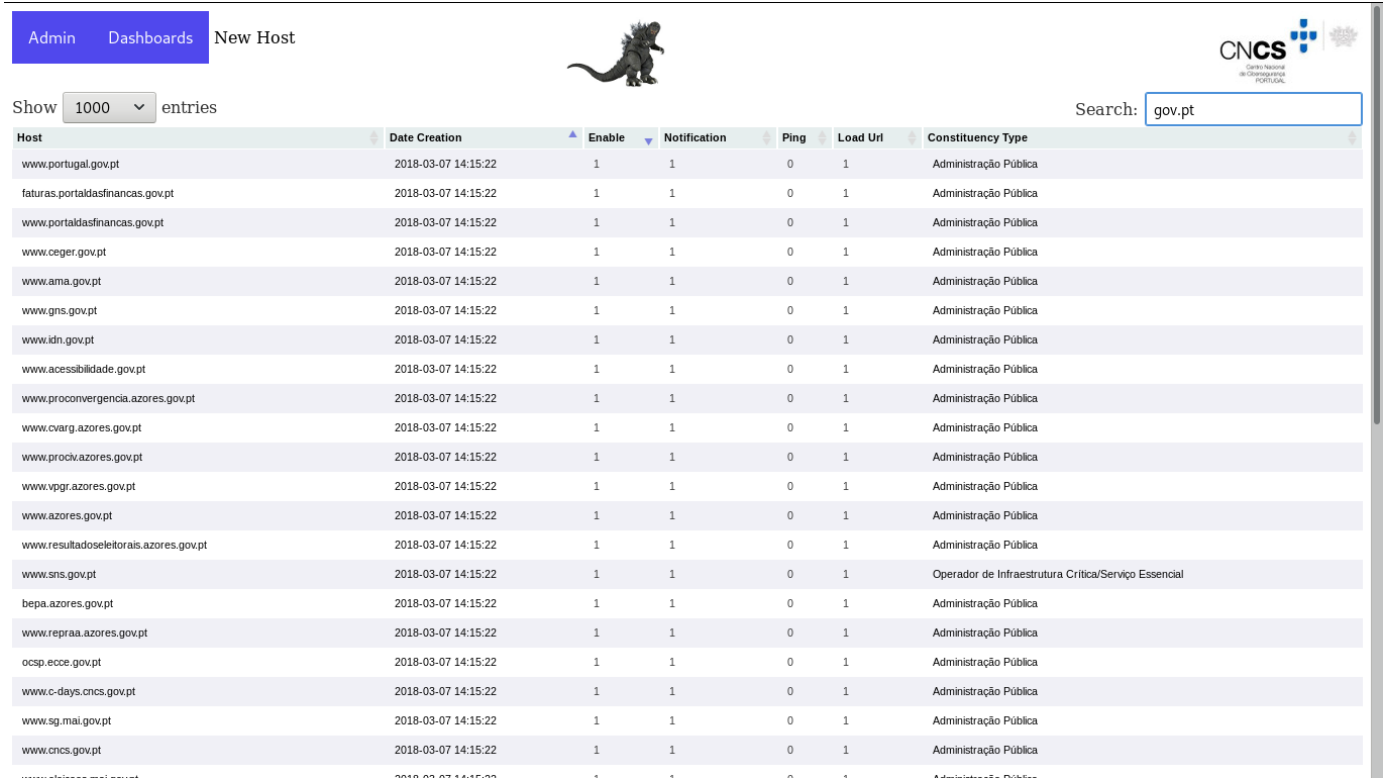
DNS

Zone: gns.gov.pt.
Last Validation: 2019-05-06 06:58:38
Total NS: 3
NS Online: ns01.cncs.gov.pt ns02.fccn.pt ns02.cncs.gov.pt
NS Offline:

PyMonitor – GodZilla: Aknowlegde Details

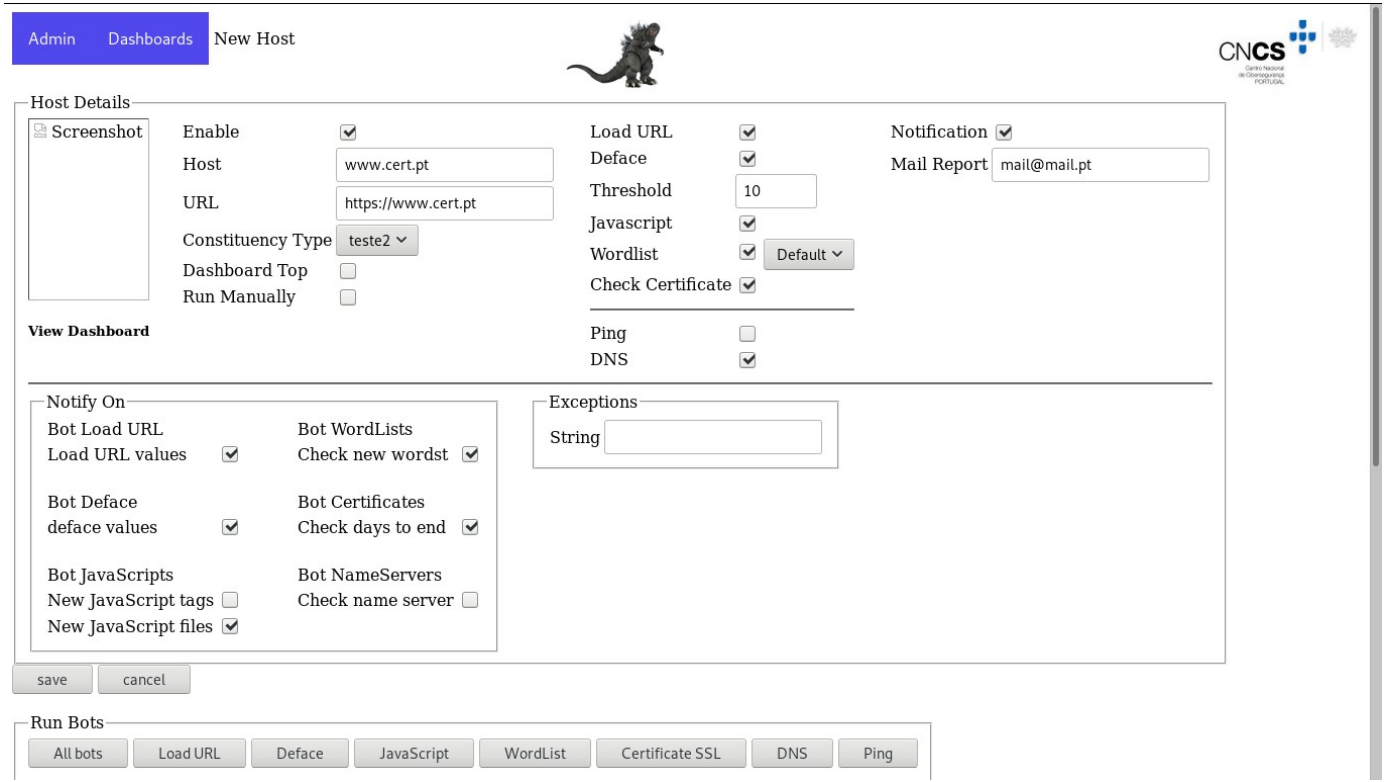


PyMonitor – GodZilla: Admin (Lista de sites/hosts)

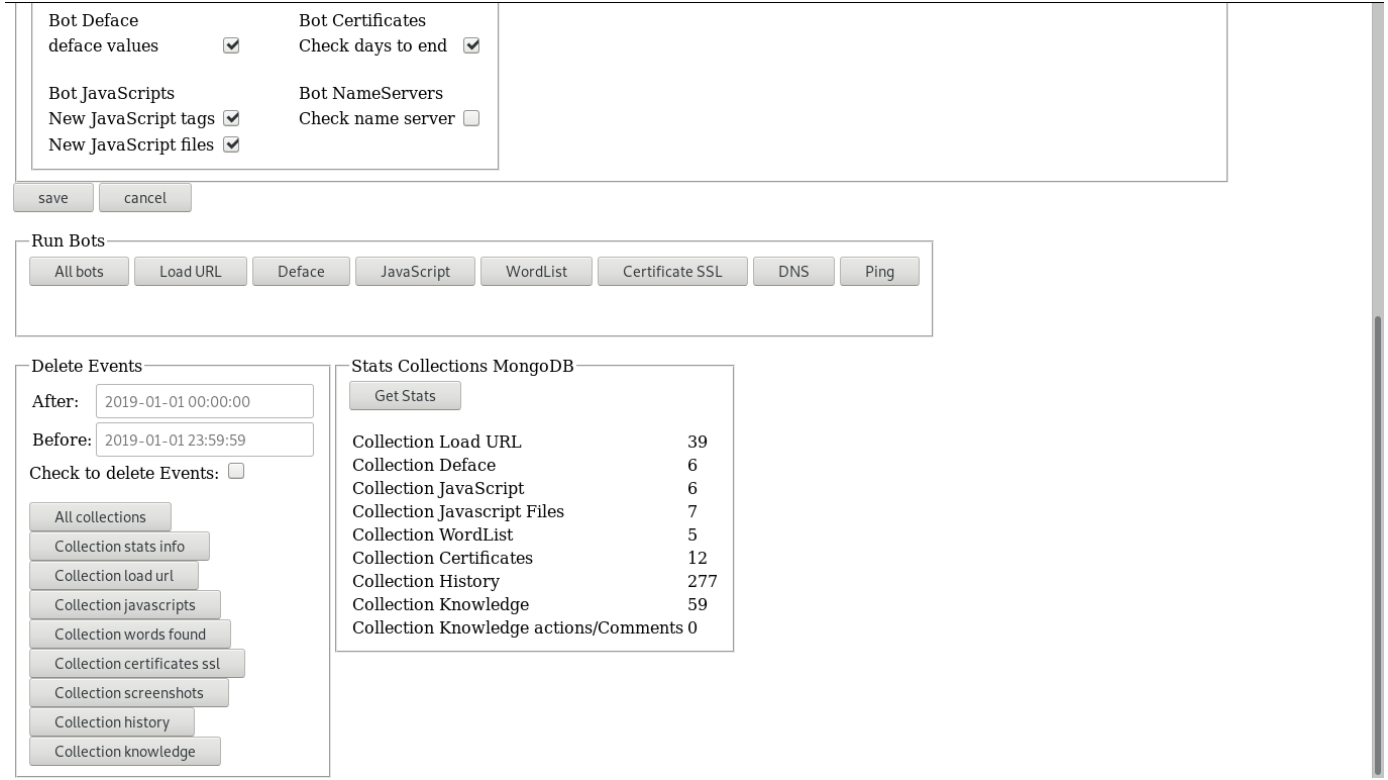


Host	Date Creation	Enable	Notification	Ping	Load Url	Constituency Type
www.portugal.gov.pt	2018-03-07 14:15:22	1	1	0	1	Administração Pública
faturas.portaldasfinancas.gov.pt	2018-03-07 14:15:22	1	1	0	1	Administração Pública
www.portaldasfinancas.gov.pt	2018-03-07 14:15:22	1	1	0	1	Administração Pública
www.ceger.gov.pt	2018-03-07 14:15:22	1	1	0	1	Administração Pública
www.ama.gov.pt	2018-03-07 14:15:22	1	1	0	1	Administração Pública
www.gns.gov.pt	2018-03-07 14:15:22	1	1	0	1	Administração Pública
www.idn.gov.pt	2018-03-07 14:15:22	1	1	0	1	Administração Pública
www.acessibilidade.gov.pt	2018-03-07 14:15:22	1	1	0	1	Administração Pública
www.proconvergencia.azores.gov.pt	2018-03-07 14:15:22	1	1	0	1	Administração Pública
www.cvarg.azores.gov.pt	2018-03-07 14:15:22	1	1	0	1	Administração Pública
www.prociv.azores.gov.pt	2018-03-07 14:15:22	1	1	0	1	Administração Pública
www.vpgr.azores.gov.pt	2018-03-07 14:15:22	1	1	0	1	Administração Pública
www.azores.gov.pt	2018-03-07 14:15:22	1	1	0	1	Administração Pública
www.resultadoseleitorais.azores.gov.pt	2018-03-07 14:15:22	1	1	0	1	Administração Pública
www.sns.gov.pt	2018-03-07 14:15:22	1	1	0	1	Operador de Infraestrutura Crítica/Serviço Essencial
bepa.azores.gov.pt	2018-03-07 14:15:22	1	1	0	1	Administração Pública
www.repraa.azores.gov.pt	2018-03-07 14:15:22	1	1	0	1	Administração Pública
ocsp.ecce.gov.pt	2018-03-07 14:15:22	1	1	0	1	Administração Pública
www.c-days.cncs.gov.pt	2018-03-07 14:15:22	1	1	0	1	Administração Pública
www.sg.mai.gov.pt	2018-03-07 14:15:22	1	1	0	1	Administração Pública
www.cncs.gov.pt	2018-03-07 14:15:22	1	1	0	1	Administração Pública

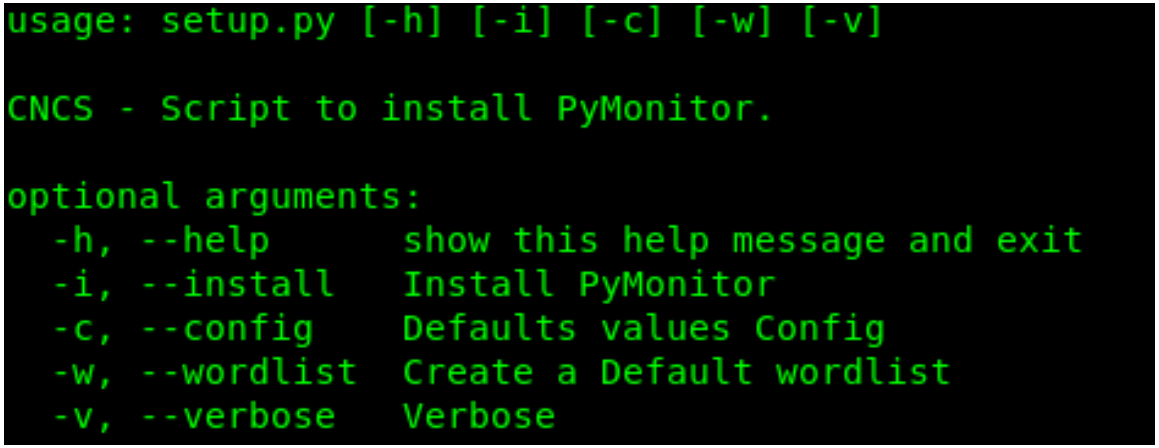
PyMonitor – GodZilla: Admin (Config. Site/Host) 1/2



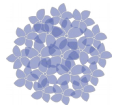
PyMonitor – GodZilla: Admin (Config. Site/Host) 2/2



PyMonitor – GodZilla: CommandLine setup.py

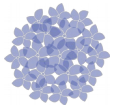


PyMonitor – GodZilla: CommandLine import.py



```
usage: import.py [-h] [-f FILEHOSTS] [-i] [-u] [-j] [-d] [-w] [-p] [-m] [-n]
                 [-l] [-v]

CNCS - Script to import hosts/urls.

optional arguments:
  -h, --help            show this help message and exit
  -f FILEHOSTS, --filehosts FILEHOSTS
                        File content hosts. Ex line: host|url|javascript|defac
                        e|wordlist|id_wordlist|ping|mail|notification|manually
                        |dns
  -i, --host            Host Name or ip address
  -u, --url             For bot LoadUrl.
  -j, --javascript      For bot JavaScript.
  -d, --deface          For Bot Deface.
  -w, --wordlist        For bot WordList. ID Wordlist
  -p, --ping            For bot ping
  -m, --mail            Mail for notification
  -n, --notification    Notification
  -l, --listwordlistids
                        List wordlist ids.
  -v, --verbose         Verbose.
```

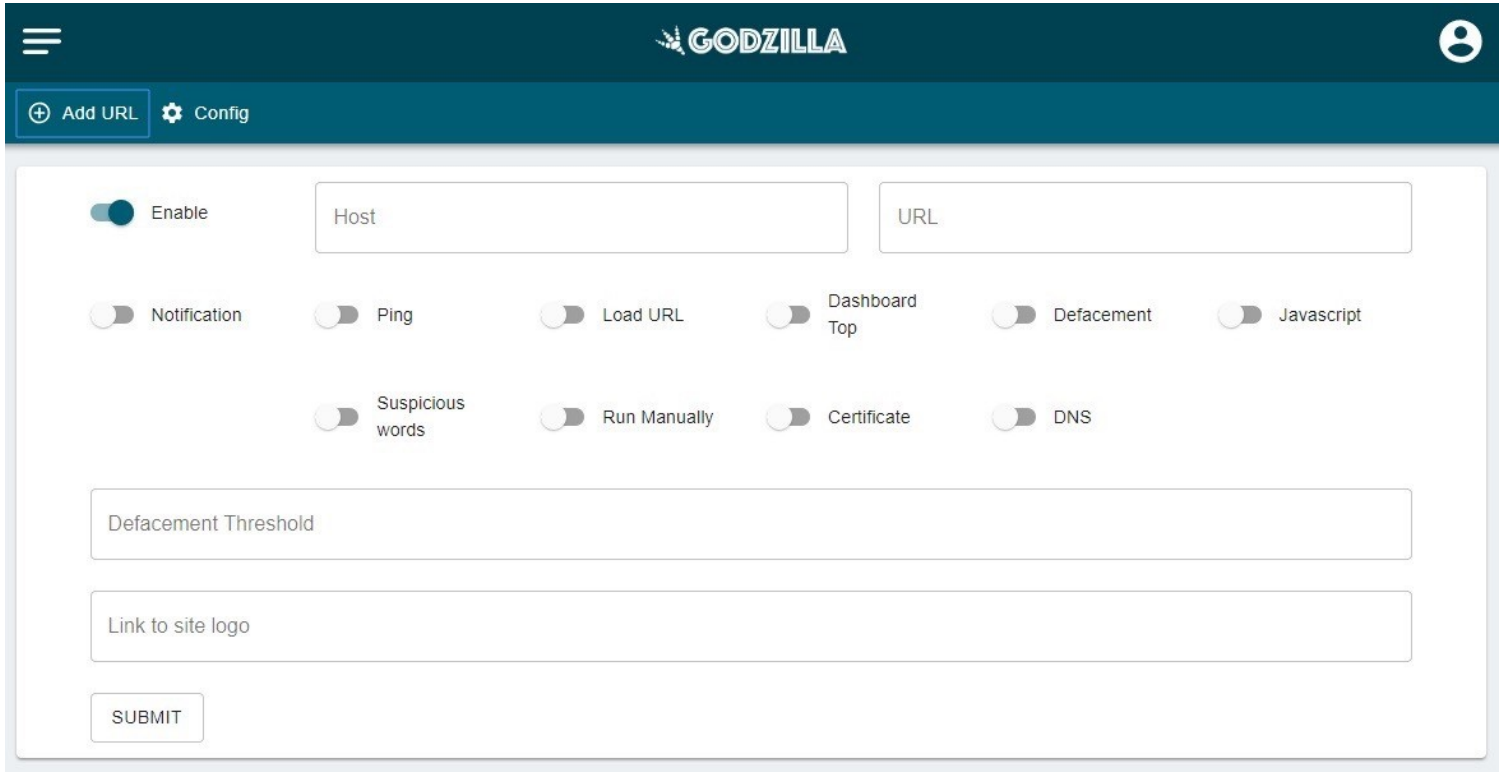
PyMonitor – GodZilla: CommandLine main.py



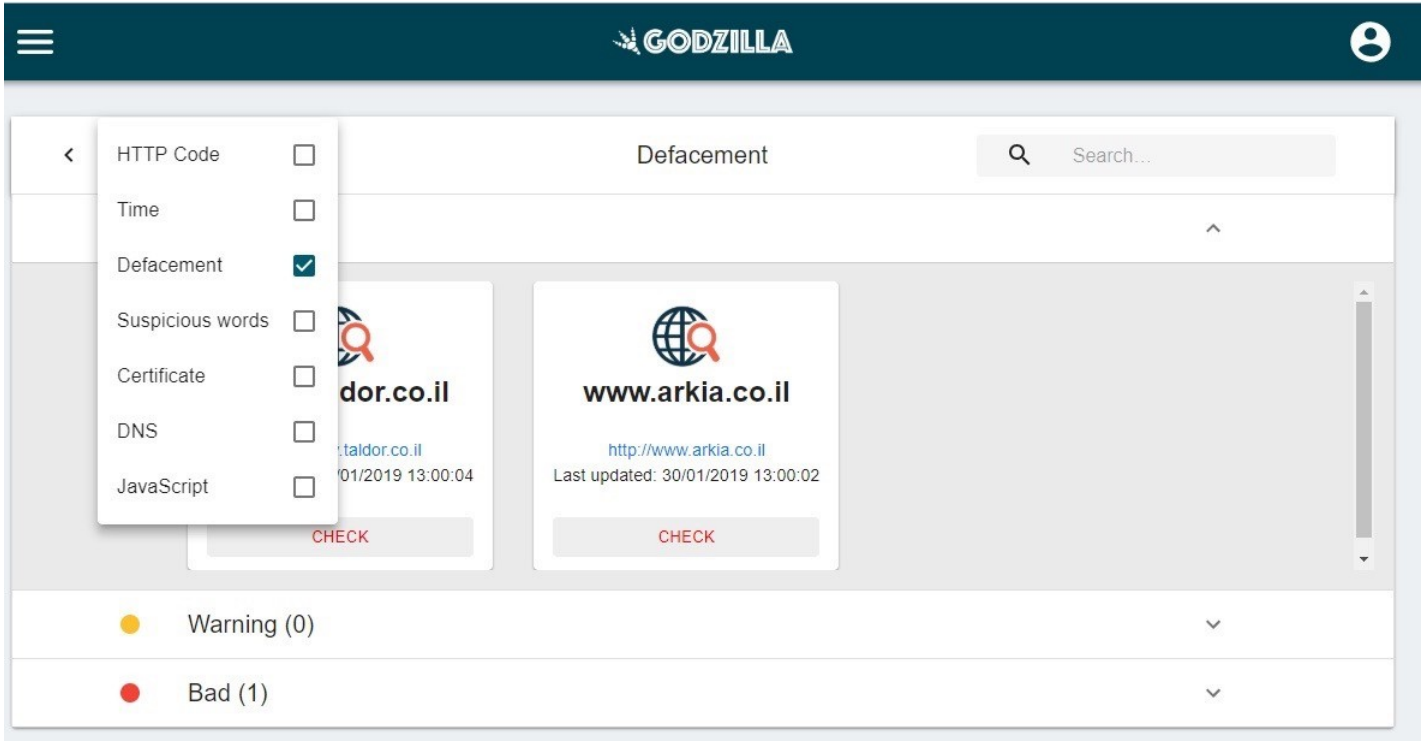
```
usage: main.py [-h] [-a] [-l] [-j] [-d] [-w] [-p] [-c] [-n] [-i ID] [-v]
               [-b LOGLEVEL]

CNCS - Script for comparare screenshots of websites.

optional arguments:
  -h, --help            show this help message and exit
  -a, --allbots         Run all bots.
  -l, --loadurl         Run bot LoadUrl.
  -j, --javascript      Run bot JavaScript.
  -d, --deface          Run Bot Deface.
  -w, --wordlist        Run bot WordList.
  -p, --ping            Run bot ping
  -c, --checkcertificate
                        Run bot Check Certificate
  -n, --dns             Run bot Check dns
  -i ID, --id ID        test a host
  -v, --verbose         Verbose.
  -b LOGLEVEL, --loglevel LOGLEVEL
                        Level log: notset, info, error, critical, debug,
                        warning
```

PyMonitor – GodZilla: Israel - Dashboard

PyMonitor – GodZilla: Israel - Admin



PyMonitor – GodZilla: Israel - Dashboard



PyMonitor – GodZilla: Perguntas

PyMonitor – GodZilla:

duarte.sousa@cncs.gov.pt