whoami

Bastian Schulz

- Teamlead Software Security
- Pentester & Bugbounty Hunter
- CTF Player

BS PAYONE

OWASP
Open Web Application
Security Project

bugcrowd

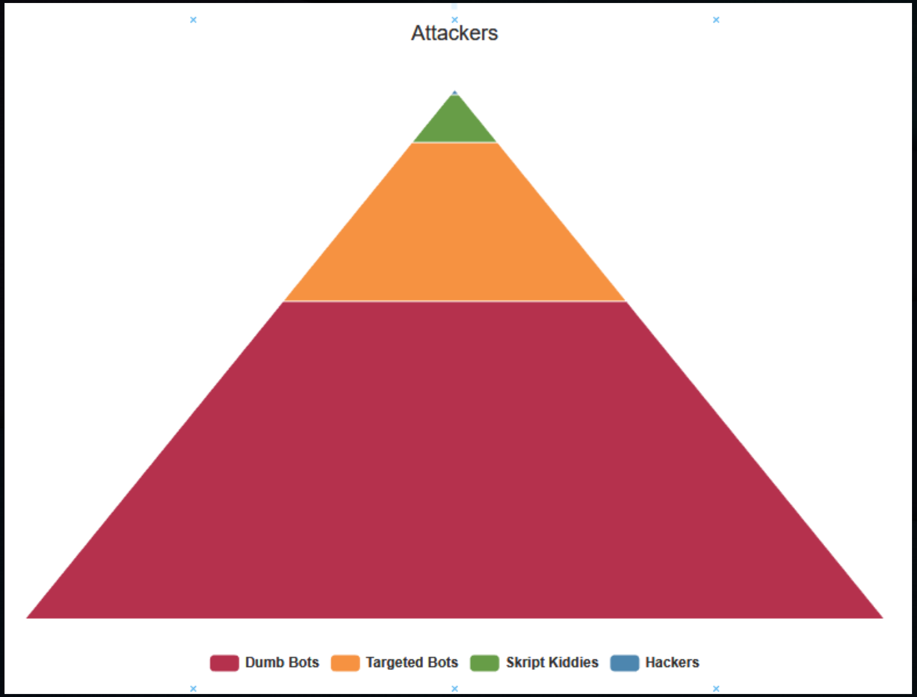
CTF TIME

hackerone

stats

- Estimated $6 trillion annually damage by 2021
- $1 cybercrime tools and kits
- >15 huge Databreaches in 2019
  - Concerned? check: https://haveibeenpwned.com/

attackers - SMB



- 60% Dumb Bots
- 30% Targeted Bots
- ~9% Skript Kiddies
- <1% Hackers

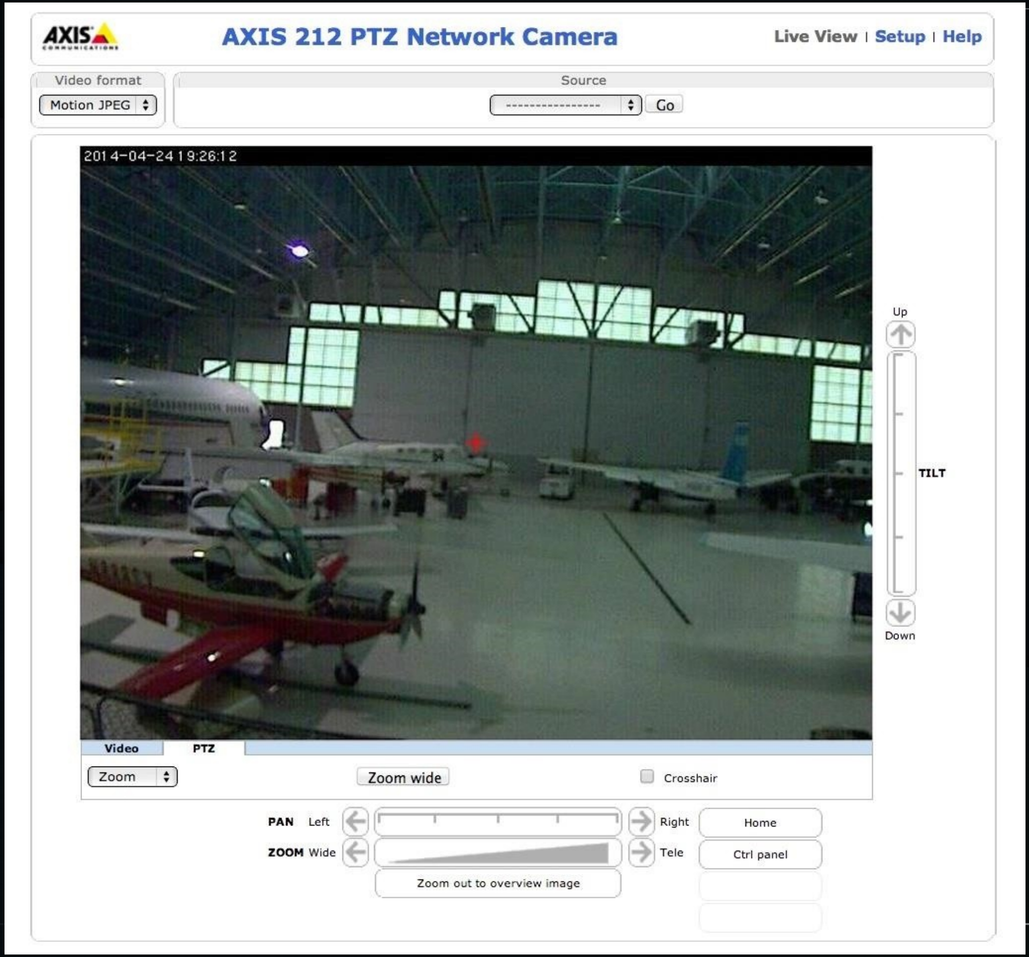
known vulnerabilies

- Public ready to use exploits
  - i.e. exploit-db.com, github …
- >1000 new vulnerabilites discovered per day

victim search

- IP Range Scanning
- Google dorks
- shodan.io
- censys.io
- ...

victim search



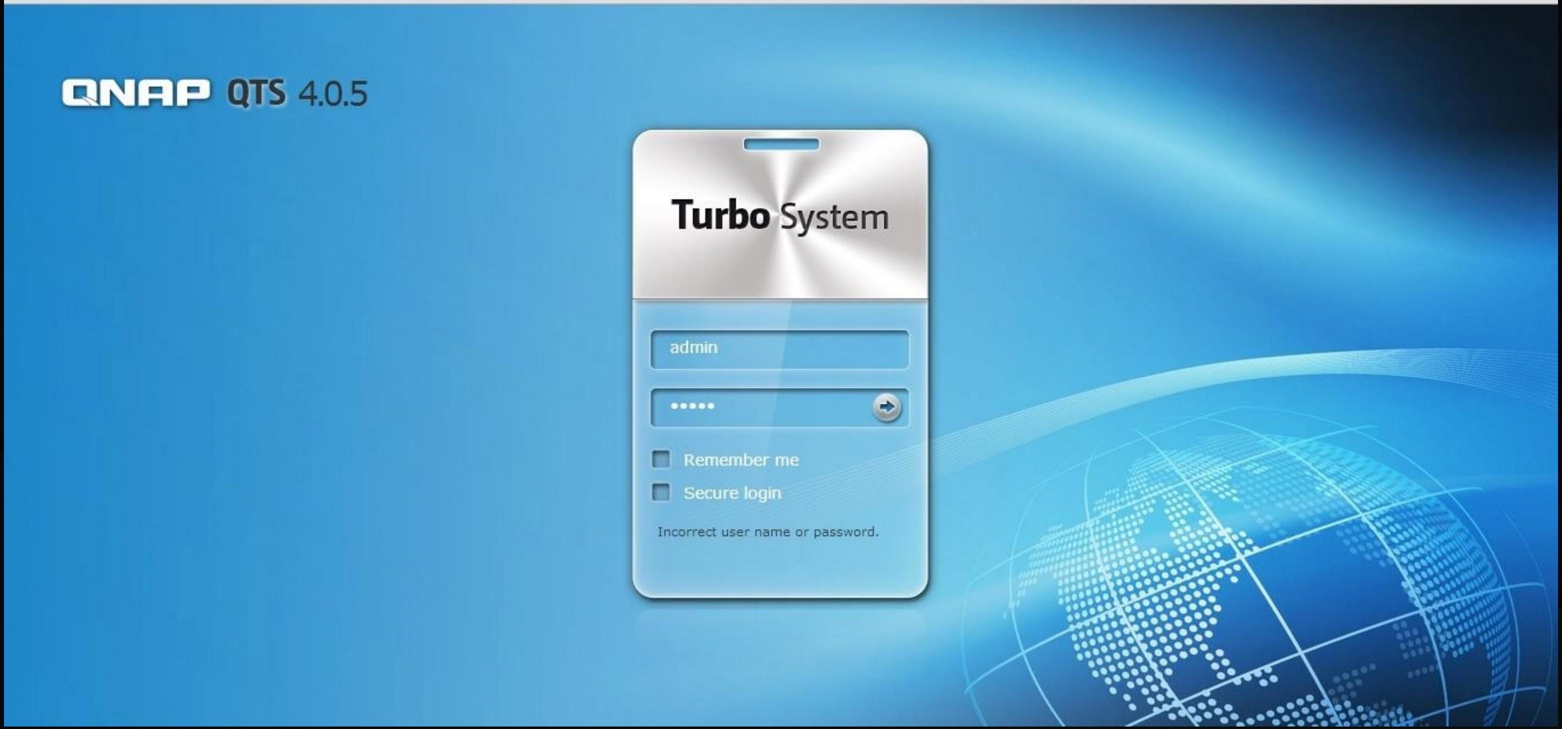
AXIS 212 PTZ Network Camera

Video format: Motion JPEG

Source: ----------------

2014-04-24 19:26:12

victim search



admin

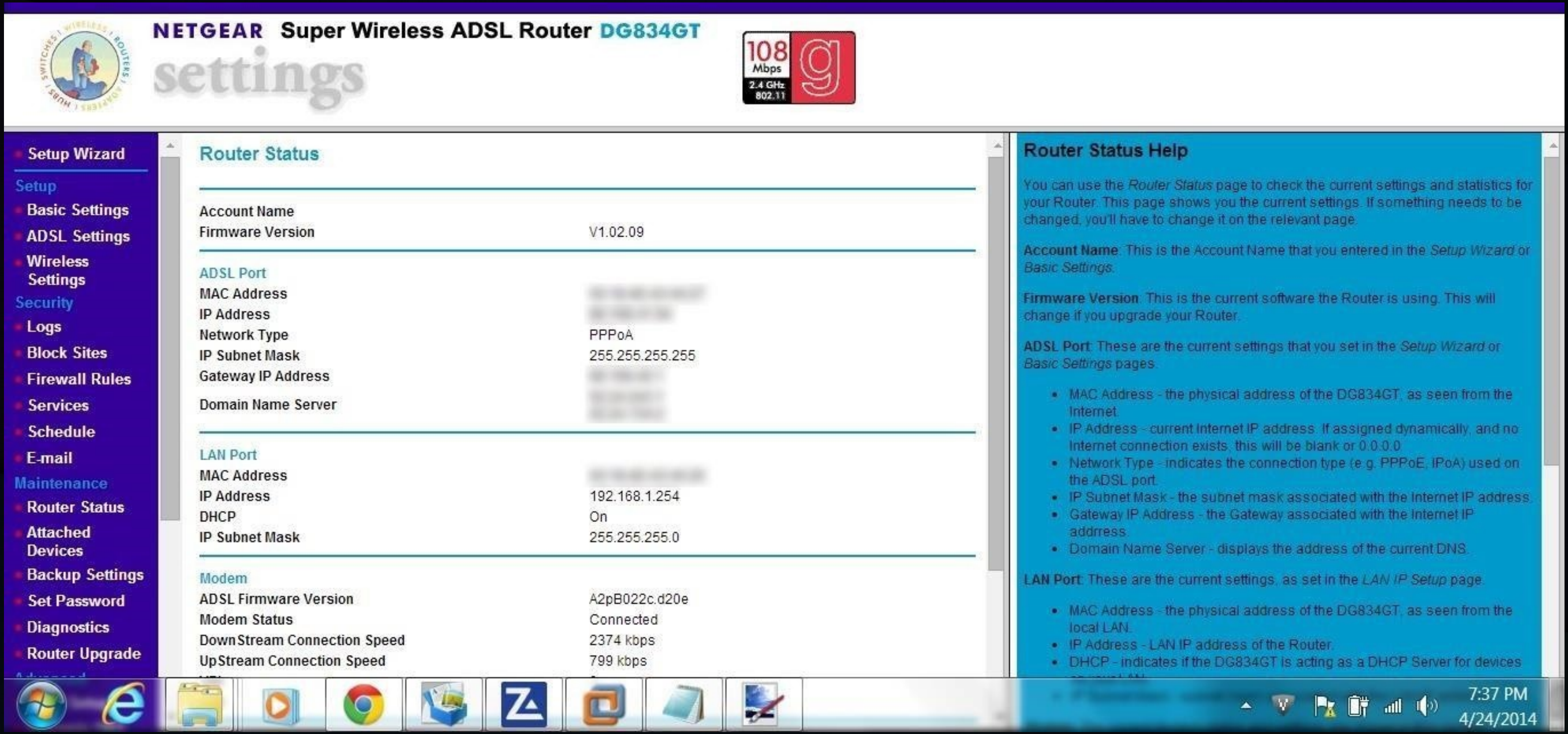
•••••

□ Remember me

□ Secure login

Incorrect user name or password.

victim search



NETGEAR Super Wireless ADSL Router DG834GT

settings

Router Status

Account Name	
Firmware Version	V1.02.09
ADSL Port	
MAC Address	[redacted]
IP Address	[redacted]
Network Type	PPPoA
IP Subnet Mask	255.255.255.255
Gateway IP Address	[redacted]
Domain Name Server	[redacted]
LAN Port	
MAC Address	[redacted]
IP Address	192.168.1.254
DHCP	On
IP Subnet Mask	255.255.255.0
Modem	
ADSL Firmware Version	A2pB022c.d20e
Modem Status	Connected
DownStream Connection Speed	2374 kbps
UpStream Connection Speed	799 kbps

Router Status Help

You can use the *Router Status* page to check the current settings and statistics for your Router. This page shows you the current settings. If something needs to be changed, you'll have to change it on the relevant page.

Account Name: This is the Account Name that you entered in the *Setup Wizard* or *Basic Settings*.

Firmware Version: This is the current software the Router is using. This will change if you upgrade your Router.

ADSL Port: These are the current settings that you set in the *Setup Wizard* or *Basic Settings* pages.

- MAC Address - the physical address of the DG834GT, as seen from the Internet.
- IP Address - current Internet IP address. If assigned dynamically, and no Internet connection exists, this will be blank or 0.0.0.0
- Network Type - indicates the connection type (e.g. PPPoE, IPoA) used on the ADSL port.
- IP Subnet Mask - the subnet mask associated with the Internet IP address.
- Gateway IP Address - the Gateway associated with the Internet IP addrress.
- Domain Name Server - displays the address of the current DNS.

LAN Port: These are the current settings, as set in the *LAN IP Setup* page.

- MAC Address - the physical address of the DG834GT, as seen from the local LAN.
- IP Address - LAN IP address of the Router.
- DHCP - indicates if the DG834GT is acting as a DHCP Server for devices

thx

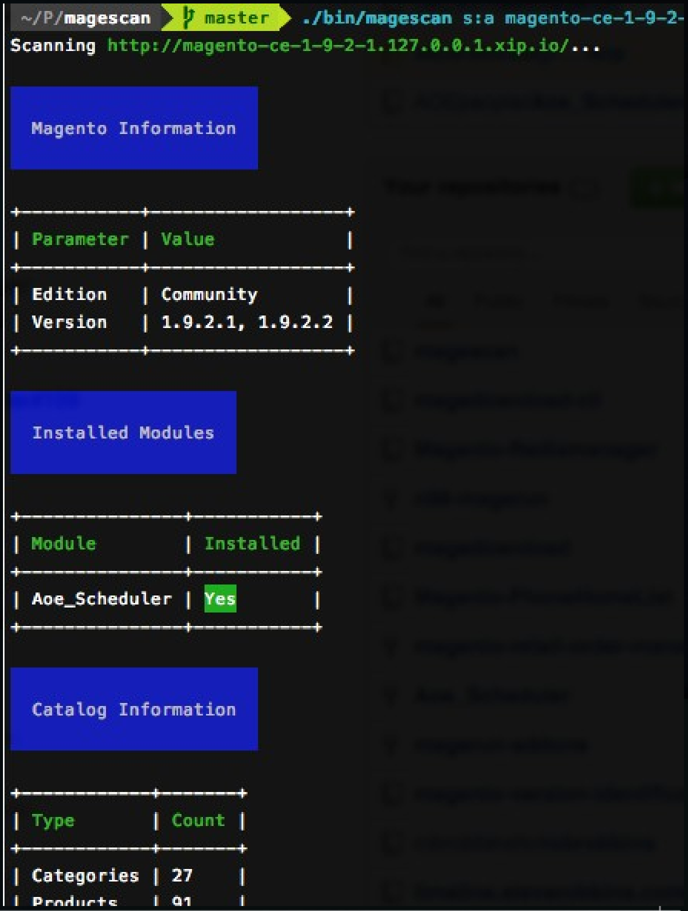
- slaxxx@protonmail.com
- Bastian.schulz@bspayone.com
- Ts3: sharkzwithlazers.pizza
- https://github.com/gexxxter
- https://github.com/gexxxter
- @bastian_schulz

tools

- Open Web Application Security Project (OWASP)
  https://www.owasp.org
- Secure Configuration Guide
  https://www.owasp.org/index.php/OWASP_Secure_Configuration_Guide

tools

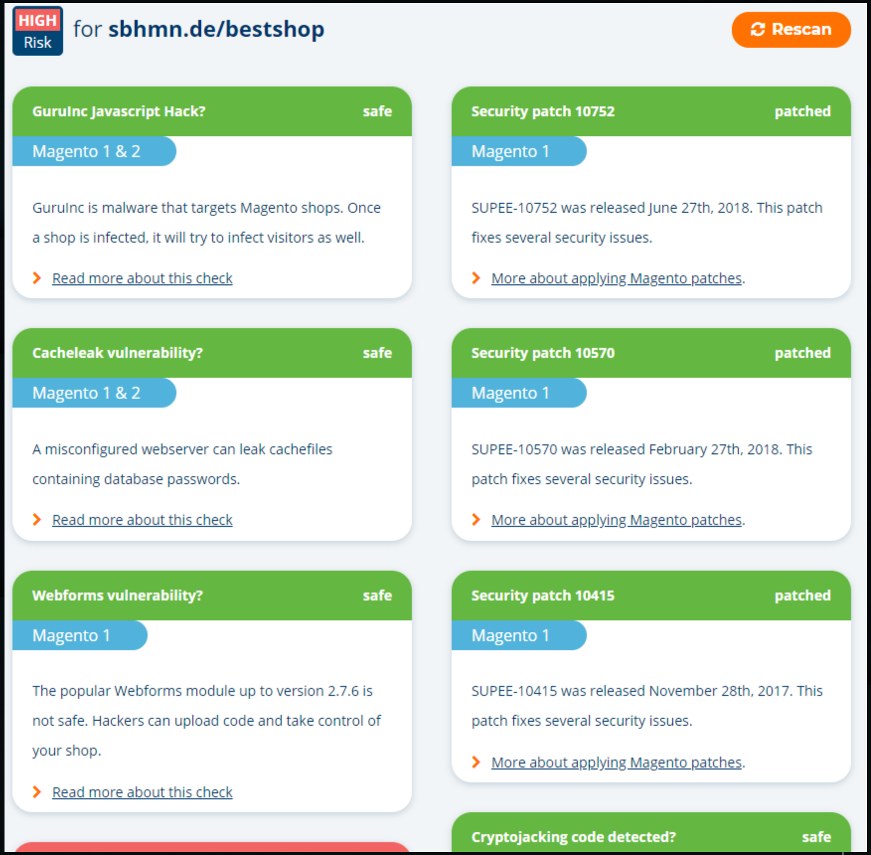
- Magescan
  https://github.com/steverobbins/magescan
- Wpscan
  https://github.com/wpscanteam/wpscan



```
~/P/magescan  master  ./bin/magescan s:a magento-ce-1-9-2-
Scanning http://magento-ce-1-9-2-1.127.0.0.1.xip.io/...

 Magento Information

+-----------+------------------+
| Parameter | Value            |
+-----------+------------------+
| Edition   | Community        |
| Version   | 1.9.2.1, 1.9.2.2 |
+-----------+------------------+

 Installed Modules

+---------------+-----------+
| Module        | Installed |
+---------------+-----------+
| Aoe_Scheduler | Yes       |
+---------------+-----------+

 Catalog Information

+------------+-------+
| Type       | Count |
+------------+-------+
| Categories | 27    |
| Products   | 91    |
```

tools

- Magereport https://www.magereport.com



for sbhmn.de/bestshop

GuruInc Javascript Hack? safe

Magento 1 & 2

GuruInc is malware that targets Magento shops. Once a shop is infected, it will try to infect visitors as well.

Read more about this check

Security patch 10752 patched

Magento 1

SUPEE-10752 was released June 27th, 2018. This patch fixes several security issues.

More about applying Magento patches.

Cacheleak vulnerability? safe

Magento 1 & 2

A misconfigured webserver can leak cachefiles containing database passwords.

Read more about this check

Security patch 10570 patched

Magento 1

SUPEE-10570 was released February 27th, 2018. This patch fixes several security issues.

More about applying Magento patches.

Webforms vulnerability? safe

Magento 1

The popular Webforms module up to version 2.7.6 is not safe. Hackers can upload code and take control of your shop.

Read more about this check

Security patch 10415 patched

Magento 1

SUPEE-10415 was released November 28th, 2017. This patch fixes several security issues.

More about applying Magento patches.

Cryptojacking code detected? safe