radware

Radware Bad-bot Vulnerability Scanner Report

XYZ INC

About Radware

We secure the Digital Experience since 1997.

10K+ CUSTOMERS

Bank of America, Capital One, ING, WELLS FARGO

ebay, STAPLES, SAMSUNG SAMSUNG SDS, Carlsberg Group

salesforce, twitter, SAP, Cisco webex

AT&T, verizon, Tech Mahindra

ANALYSTS RECOGNITION

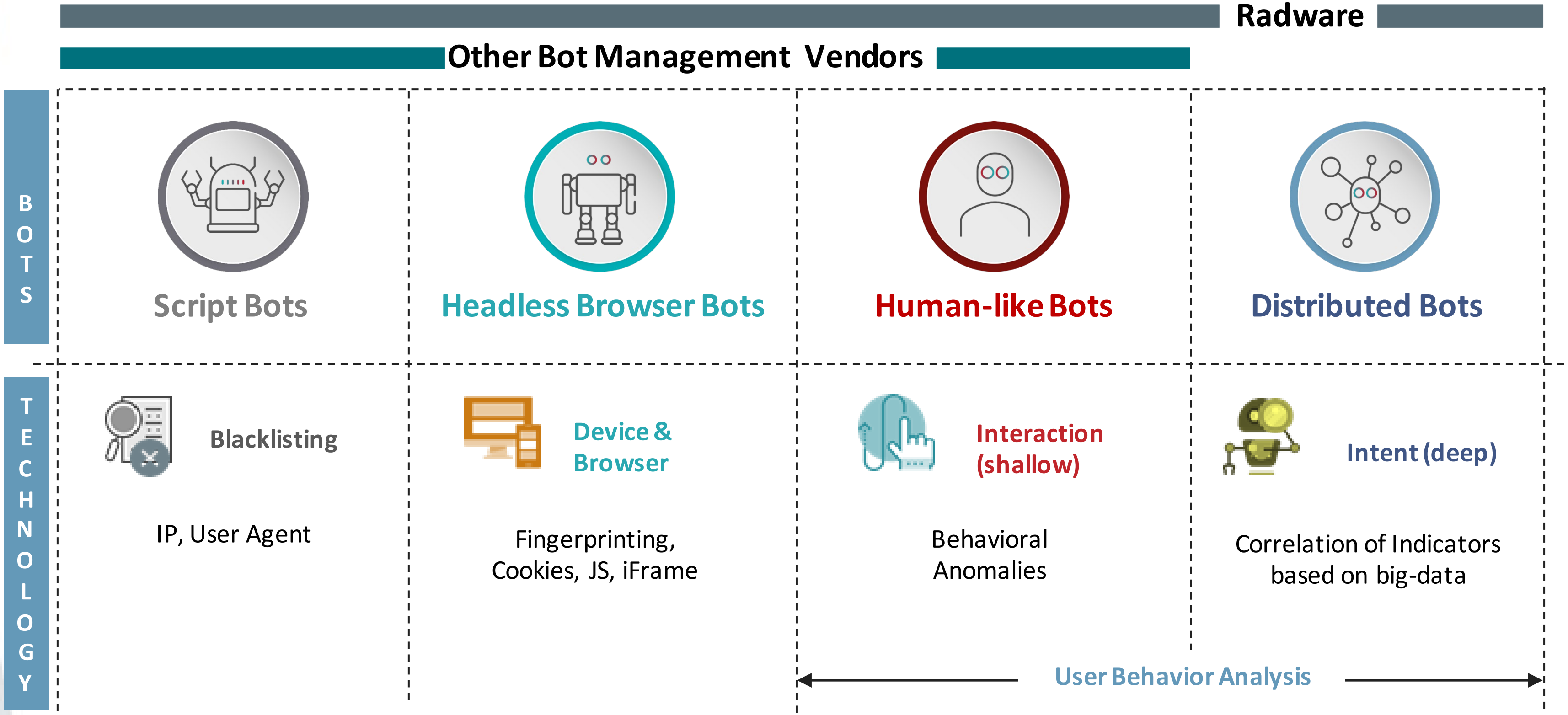
Quadrant Knowledge Solutions	Named **Leader** in **Bot Management 2020** according to SPARX MATRIX Analysis
FORRESTER	Bot Management **Leader** (2018) DDoS Wave **Leader**
Gartner	Cool Vendor **in API Economy** ADC MQ **Leader** WAF MQ **visionary**
IDC Analyze the Future	DDoS MarketSpace **#1 Leader**

OUR OEM PARTNERS

CISCO, Check Point SOFTWARE TECHNOLOGIES LTD.

Microsoft Azure, NOKIA

Bot Generation: Typical Characteristics



Radware

Other Bot Management Vendors

BOTS	Script Bots	Headless Browser Bots	Human-like Bots	Distributed Bots
TECHNOLOGY	**Blacklisting** IP, User Agent	**Device & Browser** Fingerprinting, Cookies, JS, iFrame	**Interaction (shallow)** Behavioral Anomalies	**Intent (deep)** Correlation of Indicators based on big-data

User Behavior Analysis

Summary Of Bad Bot Scanner Report

30%

Bot Attack Success Rate

GENERATION 1:

- Basic Curl Requests
- Request Package
- Wget Requests

1. Execution Time: 04/28/20 12:22 UTC
2. URL Attempted: Lacentrale.fr/
2. No of Requests: 150

85%

Bot Attack Success Rate

GENERATION 2:

- Headless Browsers
- Low and Slow
- Bot Executing JS

1. Execution Time:
   04/28/20 12:38 UTC 2.
   URL Attempted:
   Lacentrale.fr/
3. No of Requests: 150

100%

Bot Attack Success Rate

GENERATION 3:

- Distributed Attacks
- Rotating User Agents
- Session Manipulation

1. Execution Time: 04/29/20 07:37 UTC
2. URL Attempted: occasion-voiture-%audi
3. No of Requests: 150

100%

Bot Attack Success Rate

GENERATION 4:

- Human-Like Characteristics:
- Nonlinear Mouse Movement
- Low and Slow Attacks

1. Execution Time: 04/30/20 11:12 UTC
2. [redacted]
3. No of Requests: 20

The purpose of this exercise is to find vulnerabilities of your website which may expose your content to different types of bot attacks. The content obtained from your website by Radware Bot Manager is used purely for analysis and tests described in this report. The data will not be used in any way that may harm or hinder your business activity.

Generation 1 Bots: Attack Vectors

First-generation bots are built with ***basic scripting tools*** and make cURL-like requests to websites using a specific set of IP addresses (often just one or two). Typically a data center IP is used to repeatedly targeted a section in a uniform programmatic pattern. These attacks are easy to detect and whitelist as the UA typically is not spoofed to conceal the browser characteristics and. Blacklisting the IP or the UA typically will resolve such an issue. Gen 1 Bots typically cannot maintain the sessions or execute a JS.

Targeted URL: [redacted]

Check your Server Logs / Time: 04/28/20 12:22:22 UTC

curl://

How did your site respond to bots generated from cURL ?
Result: FAIL

```
[~]$ wget
```

How did your site respond to bots generated from wget?
Result: FAIL

Requests

How did your site respond to bots generated from Scrapy?
Result: FAIL

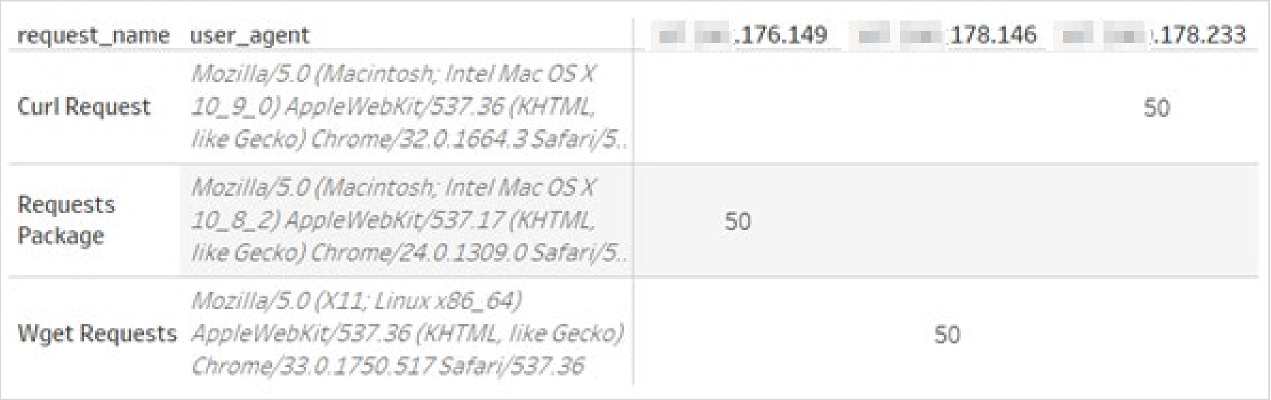
Generation 1 Bots: Vulnerability

VULNERABILITY STATUS HIGH RISK

Attempt 1:
Request Frequency: 1s
Total Requests Made: 5
Bypassed: 5
Response Code: 200

cURL Request → Data Center IP → **5/5** Requests Bypassed

Attempt 2:
Request Frequency: 1s
Total Requests Made: 150
Bypassed: 150
Response Code: 200



request_name	user_agent	[redacted].176.149	[redacted].178.146	[redacted].178.233
Curl Request	*Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1664.3 Safari/5..*			50
Requests Package	*Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_2) AppleWebKit/537.17 (KHTML, like Gecko) Chrome/24.0.1309.0 Safari/5..*	50		
Wget Requests	*Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.517 Safari/537.36*		50	

Generation 2 Bots: Attack Vectors

These bots operate through website development and ***testing tools known as "headless" browsers*** (examples: PhantomJS and SimpleBrowser), as well as later versions of Chrome and Firefox, which allow for operation in headless mode. These bots coupled with spoofed user agents are typically able to bypass generic WAF solutions. Selenium bots typically maintain sessions and they could be used to attack targeted sections with specific intent like Price scraping or an Account takeover attack.

Targeted URL: [redacted]

Check your Server Logs/Time: 04/28/20 12:38:59 UTC

IPs Used: DCH & Proxy IPs

How did your site respond to bots generated from Selenium ?
Result: FAIL

How did your site respond to bots generated from PhantomJS?
Result: FAIL

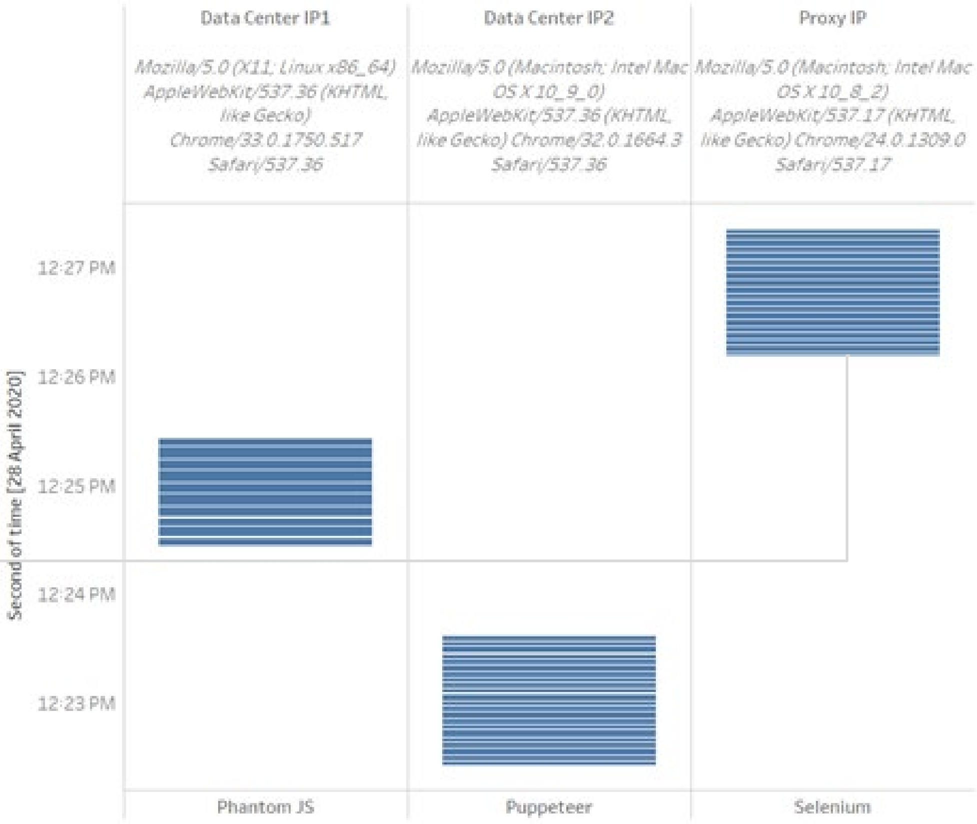
How did your site respond to bots generated from Puppeteer?
Result: PASS

Generation 2 Bots: Vulnerability

VULNERABILITY STATUS: HIGH RISK

Attempt Scenario:
Request Frequency: 1s
Total Requests Made: 150 Requests
Bypassed: 135
Response Code Served for Block: 403
Response Code Served for Pass: 200

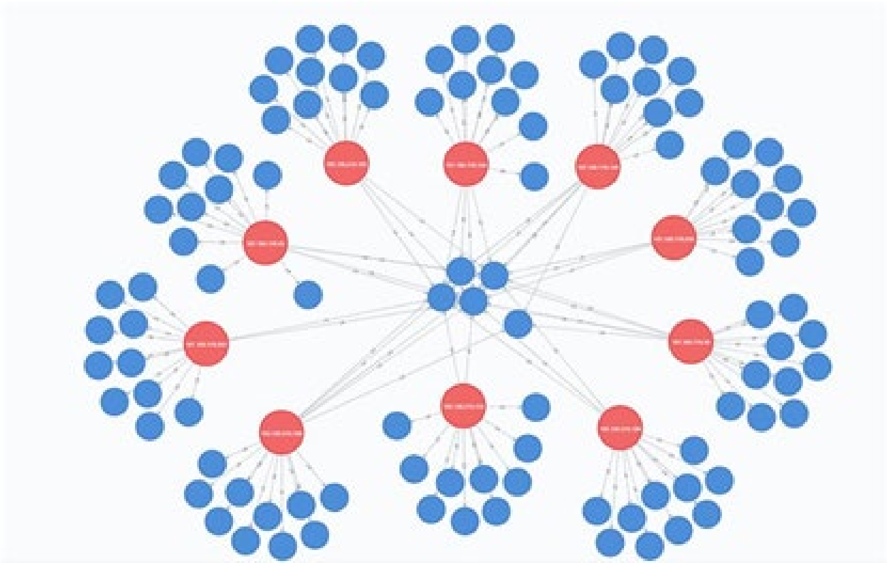
Each line represents an attack in the mentioned time frame. Color Code highlighted mentioned if the request was allowed or blocked.



Response Code
🟦 200

Generation 3 Bots - Typical Attack Pattern

These bots typically simulate basic human-like interactions, such as relevant sectional navigation. They also originate from distributed IPs alternating with multiple user agents. This combination of these attack vectors makes it difficult to fingerprint and detect such bot hits. However, Gen 3 Bots fail to demonstrate human-like randomness in their behavior.



Attempt Scenario:
URL Targeted:

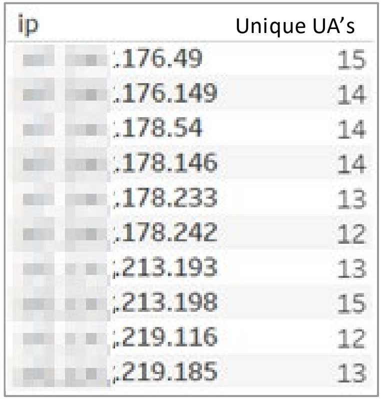
[redacted]

Request Frequency: 3s
Total Requests Made: 100 Requests

Mentioned above is a depiction of attack scenario performed through our internal tool. Basically, 100 requests are to be made alternating between a fixed set of IPs and User Agents at a fixed interval of time. Attacks would be targeted using headless browsers like Phantomjs or Puppeteer.

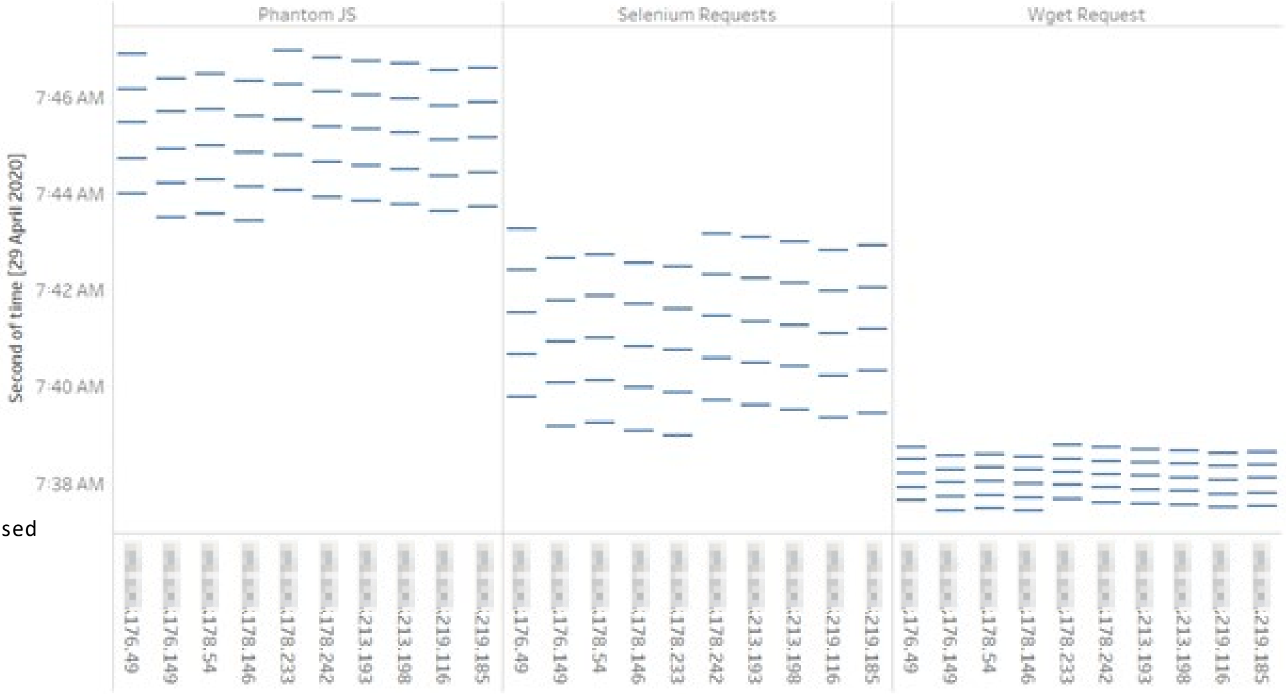
Generation 3 Bots - Distributed Attacks

VULNERABILITY STATUS: HIGH RISK



ip	Unique UA's
[redacted].176.49	15
[redacted].176.149	14
[redacted].178.54	14
[redacted].178.146	14
[redacted].178.233	13
[redacted].178.242	12
[redacted].213.193	13
[redacted].213.198	15
[redacted].219.116	12
[redacted].219.185	13

Rotating UA's Used



Rotating IPs Used

Generation 4 Bots Human Like Characteristics

4th Generation Bots, apart from the fact they are typically distributed and make minimal hits to remain well below the radar, mimic/replicate human traversal across sections that are difficult to differentiate

Following Tests have been conducted to evaluate if your site is able to block bots that execute Javascript events having a ***Randomised movement, Element Clicks*** and ***Keystrokes*** that resemble human behaviour.

Mouse Movements

No of of Attack Requests: **15**
Time of Attack:
Attack Vector: Distributed IPs
Successful Bypass: **YES**

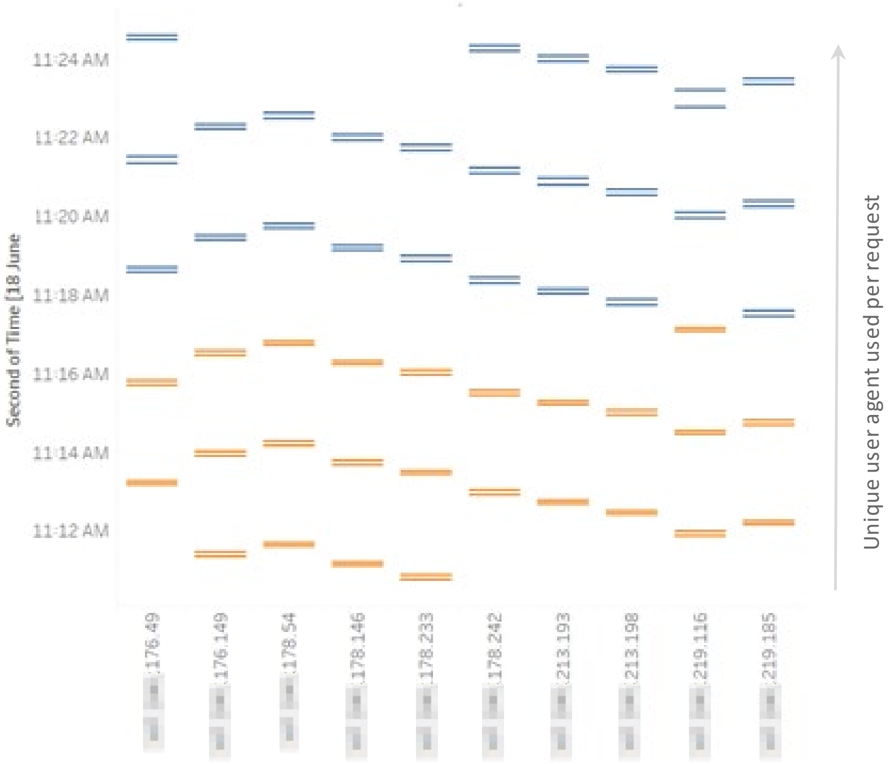
Keystrokes

No of of Attack Requests: **15**
Time of Attack:
Attack Vector: Distributed IPs
Successful Bypass: **YES**

Zoom In/Out

No of of Attack Requests: **10**
Time of Attack:
Attack Vector: Distributed IPs
Successful Bypass: **YES**

Generation 4 Bots - Low And Slow Attacks



Generation 4 bots hit your servers at *periodic/timed intervals* (using distributed IPs & user agents) with minimum requests to ensure the requests are not captured/traced for bot signature creation.

Also, gen4 bots exhibit '*human like behaviour*' considering their website navigation and traversal.

Request Name
🟦 Phantom_JS Requests
🟧 Selenium Requests

Attempt scenario:
Time span: 12 minutes
URL attempt:

[redacted]

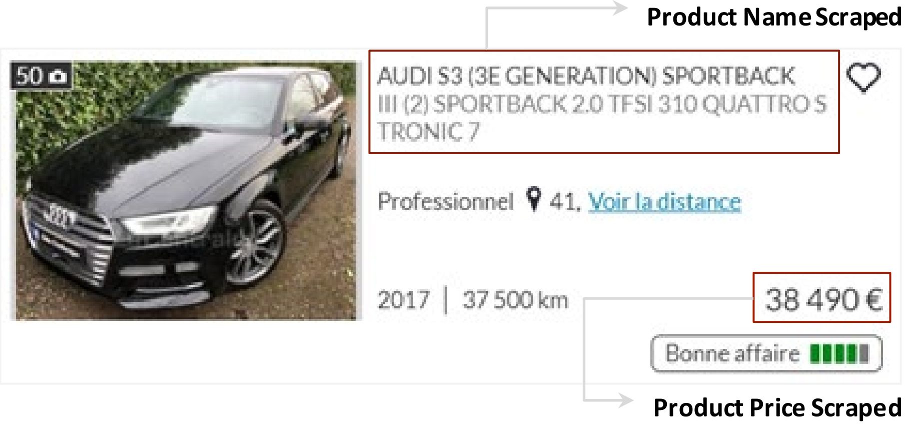
Total requests made: 100 requests
Bypassed: 135
Response code served for pass: 200

Potential Vulnerabilities On Your Platform

Primary Listings Scraped	Requests Bypassed	Risk Level
Product Listing Page - Price Scraping	150	**Critical**
Product Detail Page - Content Scraping	150	**Critical**
AJAX Calls on Product Pages	10	**High**

Scraping Dynamic Prices Of Your Products

URL Targeted: [redacted]
Time of Attack: 04/29/20 08:12:06 UTC
No of Hits Made / Requests Bypassed: 50 Requests Made / 50 Requests Allowed



AUDI S3 (3E GENERATION) SPORTBACK III (2) SPORTBACK 2.0 TFSI 310 QUATTRO S TRONIC 7

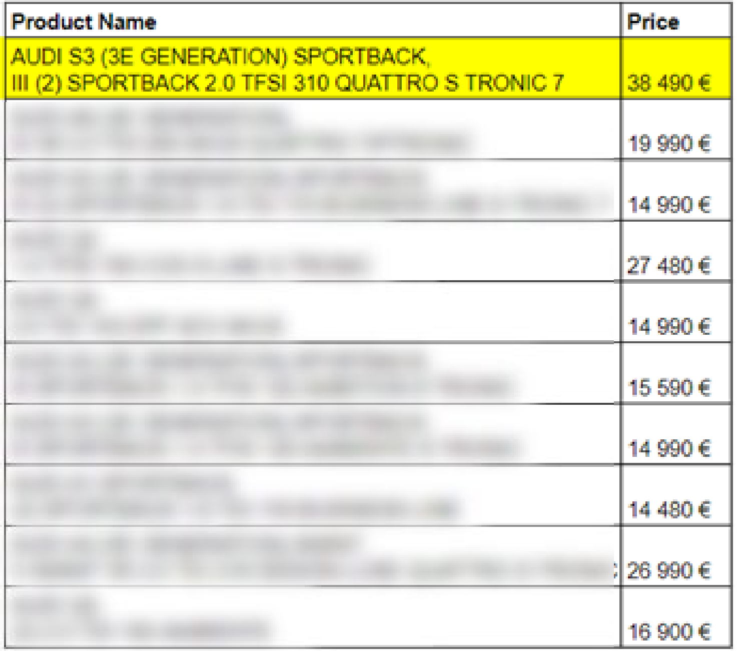
Professionnel 41, Voir la distance

2017 | 37 500 km

38 490 €

Bonne affaire

Scrape Results: Product Name and Prices Scraped



Product Name	Price
AUDI S3 (3E GENERATION) SPORTBACK, III (2) SPORTBACK 2.0 TFSI 310 QUATTRO S TRONIC 7	38 490 €
[redacted]	19 990 €
[redacted]	14 990 €
[redacted]	27 480 €
[redacted]	14 990 €
[redacted]	15 590 €
[redacted]	14 990 €
[redacted]	14 480 €
[redacted]	26 990 €
[redacted]	16 900 €

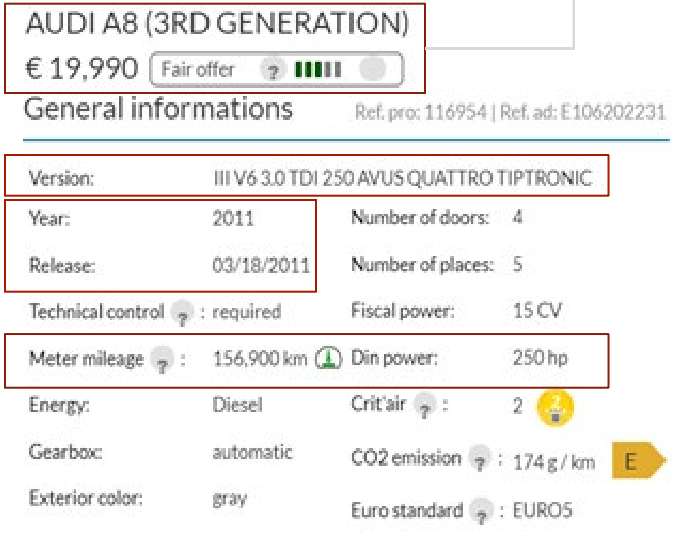
X-Path Patterns Extracted

Targeted Content: "//div[@class='adLineContainer']"
Pagination: "//div[@class='rch-pagination']//li[12]//a/@href"
Product Name: ".//div[@class='subContRight']/h3/span"
Product Price: ".//div[@class='fieldPrice']/nobr//span[2]"

Sniffing Individual Product Level Details!

URL Targeted: [redacted]
Time of Attack: 04/29/20 09:10:06 UTC
No of Hits Made / Requests Bypassed: 50 Requests Made / 50 Requests Allowed

Highlighted Product Details are getting Scraped



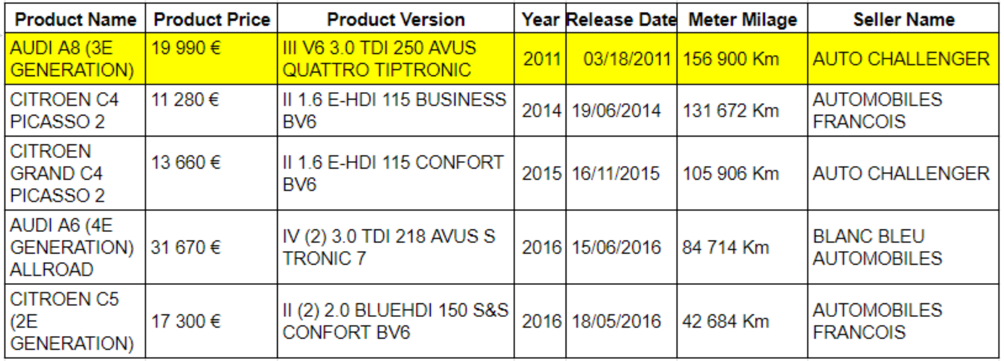
AUDI A8 (3RD GENERATION)

€ 19,990 Fair offer

General informations Ref. pro: 116954 | Ref. ad: E106202231

Version:	III V6 3.0 TDI 250 AVUS QUATTRO TIPTRONIC		
Year:	2011	Number of doors:	4
Release:	03/18/2011	Number of places:	5
Technical control :	required	Fiscal power:	15 CV
Meter mileage :	156,900 km	Din power:	250 hp
Energy:	Diesel	Crit'air :	2
Gearbox:	automatic	CO2 emission :	174 g / km E
Exterior color:	gray	Euro standard :	EURO5

Individual Product Details Product Details Scraped



Product Name	Product Price	Product Version	Year	Release Date	Meter Milage	Seller Name
AUDI A8 (3E GENERATION)	19 990 €	III V6 3.0 TDI 250 AVUS QUATTRO TIPTRONIC	2011	03/18/2011	156 900 Km	AUTO CHALLENGER
CITROEN C4 PICASSO 2	11 280 €	II 1.6 E-HDI 115 BUSINESS BV6	2014	19/06/2014	131 672 Km	AUTOMOBILES FRANCOIS
CITROEN GRAND C4 PICASSO 2	13 660 €	II 1.6 E-HDI 115 CONFORT BV6	2015	16/11/2015	105 906 Km	AUTO CHALLENGER
AUDI A6 (4E GENERATION) ALLROAD	31 670 €	IV (2) 3.0 TDI 218 AVUS S TRONIC 7	2016	15/06/2016	84 714 Km	BLANC BLEU AUTOMOBILES
CITROEN C5 (2E GENERATION)	17 300 €	II (2) 2.0 BLUEHDI 150 S&S CONFORT BV6	2016	18/05/2016	42 684 Km	AUTOMOBILES FRANCOIS

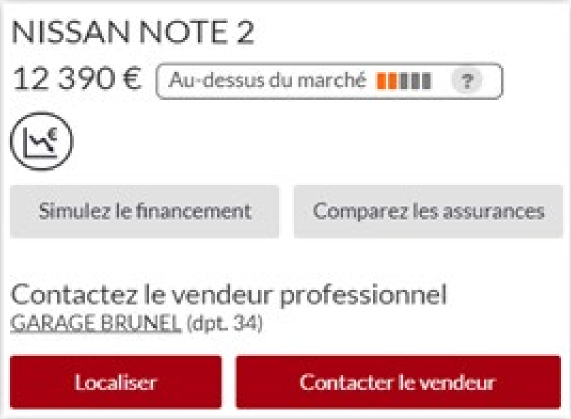
X-Path Patterns Extracted:

Product Name: "//div[@class='cbm-mainInfos']/h1"
Product Price: "//span[@class='cbm__priceWrapper']"
Version: //li[@class='cbm-allCols']//span[2]
Year: "//div[@class='cbm-moduleInfos__informationList']//li[1]//span[2]"
Seller: "//div[@class='cbm-moduleInfos__informationList']//li[2]//span[2]"
Mileage:"//div[@class='cbm-moduleInfos__informationList']//li[4]//span[2]"

Leaking Information From Your JS-Ajax Calls

Time of Attack: 04/29/20 09:10:06 UTC
No of Hits Made / Requests Bypassed: 10 Requests

URL: [redacted]



NISSAN NOTE 2

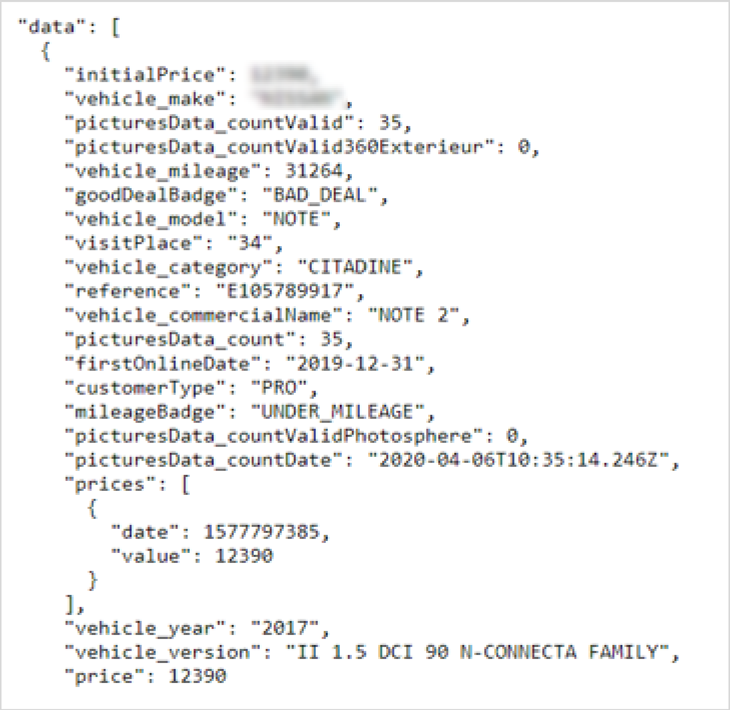
12 390 €

Contactez le vendeur professionnel

GARAGE BRUNEL (dpt. 34)

AJAX CALL URL: [redacted]

JSON with the Product Detail Scrapped



```
"data": [
  {
    "initialPrice": [redacted],
    "vehicle_make": [redacted],
    "picturesData_countValid": 35,
    "picturesData_countValid360Exterieur": 0,
    "vehicle_mileage": 31264,
    "goodDealBadge": "BAD_DEAL",
    "vehicle_model": "NOTE",
    "visitPlace": "34",
    "vehicle_category": "CITADINE",
    "reference": "E105789917",
    "vehicle_commercialName": "NOTE 2",
    "picturesData_count": 35,
    "firstOnlineDate": "2019-12-31",
    "customerType": "PRO",
    "mileageBadge": "UNDER_MILEAGE",
    "picturesData_countValidPhotosphere": 0,
    "picturesData_countDate": "2020-04-06T10:35:14.246Z",
    "prices": [
      {
        "date": 1577797385,
        "value": 12390
      }
    ],
    "vehicle_year": "2017",
    "vehicle_version": "II 1.5 DCI 90 N-CONNECTA FAMILY",
    "price": 12390
```

Industry Recognition

Notable Vendor in Hype Cycle for Application Security, 2018

Gartner.

2018 Global Bot Risk Management Customer Value Leadership Award

FROST & SULLIVAN

Positioned As A 'Late Stage' Vendor In New Tech: Bot Management, 2018

FORRESTER®

Representative vendor in 'Protecting Web Apps & APIs from Exploits & Abuse' Report

Gartner.

Compliance

PCI DSS
COMPLIANT

HIPAA

INFORMATION SECURITY MANAGEMENT SYSTEMS
ISO
ISO/IEC 27001:2013

radware

Thank You!