



AssassinGo



AssassinGo

AssassinGo is an extensible and concurrency information gathering and vulnerability scanning framework, with WebSocket based Web GUI.

Just for learn, welcome PR.

Features

- ☑ Retrieve Security Headers
- ☑ Bypass CloudFlare
- ☑ Detect CMS Version
- ☑ Honeypot Detect
- ☑ Port Scan
- ☑ Trace Route and Mark on Google Map
- ☑ Subdomain Scan
- ☑ Dir Scan and Site Map
- ☑ Whois Lookup
- ☑ Crawl the Paramed URLs
- ☑ Basic SQLi Check
- ☑ Basic XSS Check
- ☑ Intruder
- ☑ SSH Bruter
- ☑ Google-Hacking with Headless-Chrome

- ☒ Friendly PoC Interface
- ☒ Web GUI(using WebSocket)
- ☐ Generate Report

Installation

localhost

```
1 git clone https://github.com/AmyangXYZ/AssassinGo
2 cd AssassinGo
3 docker-compose up --build -d
4 cat backup.sql | docker exec -i assassingo_mariadb_1 /usr/bin/mysql -
  uag --password=password ag
```

Then visit <http://127.0.0.1:8000> and login as admin:admin

VPS

If you want to deploy on your VPS, please clone the Frontend and modify the `base_url` of AJAX and WebSocket, then run `npm run build` and copy the output to `web/` directory as `deploy.sh` says.

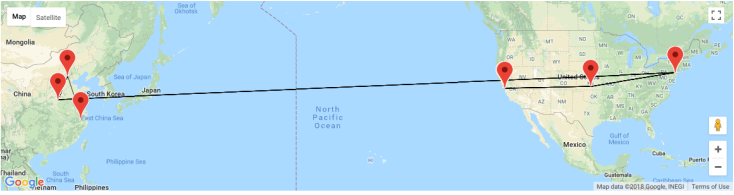
Remember to add your google-map key in `index.html`.

Demo

The screenshot displays the AssassinGo web interface. On the left is a sidebar with navigation icons: Home, Recon, Attack, Assassinate, and Seek. The main content area shows a 'Recon' report for the domain 'upwork.com'. The report includes a 'Honeypot Score' of 30%, IP address 104.16.33.27, Server: cloudflare, CMS: Unknown, and RealIP: 54.241.153.177. The report is divided into three sections: 'Whois', 'Security Header', and 'Port Scan'. The 'Whois' section shows domain details for upwork.com, including registrar MarkMonitor, Inc., creation date 2002-01-30T05:10:35-0800, expiration date 2020-01-30T00:00:00-0800, and DNS information. The 'Security Header' section lists various security headers and their status: Click-Jacking Protection (checked), Content-Security-Policy (unchecked), Strict Transport Security (unchecked), and X-Content-Type-Options (checked). The 'Port Scan' section shows a table of open ports and services: Port 80 (http), Port 443 (https), Port 8080 (httpproxy), and Port 8443 (httpsalt). At the bottom of the interface, there are links for Base, TraceRoute, Sitemap, Dirb, and Subdomain.

Recon

traceroute



TTL	ADDR	ELAPSED TIME	COUNTRY	LATITUDE	LONGITUDE
1	172.18.0.1	171735		0	0
2	0.0.0.0	0		0	0
3	45.63.81.33	18471802	United States	37.3338	-121.8915
4	0.0.0.0	0		0	0
5	4.7.18.205	1602080	United States	37.3013	-121.8079


Base TraceRoute Sitemap Dirb Subdomain

Recon

subdomain

499	law.qq.com
500	dav.qq.com
501	storm.qq.com
502	sns.qq.com
503	wan.qq.com
504	shell.qq.com
505	at.qq.com
506	golf.qq.com
507	city.qq.com
508	sky.qq.com
509	gp.qq.com
510	journal.qq.com

Base TraceRoute Sitemap Dirb Subdomain



AssassinGo

Home

Recon

Attack

Assassinate

Seek

Attack

intruder

#	PAYLOAD	STATUS	LENGTH
1995	631	200	3
1996	243	200	3
1997	905	200	3
1998	773	200	3
1999	750	200	3
2000	470	200	3
2001	761	200	3
2002	476	200	3
2003	495	200	3
2004	811	200	3
2005	803	200	3
2006	403	200	3


GET /test.php?id=\$\$1\$\$ HTTP/1.1
Host: 47.94.136.141:8888

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17

1000

DOSTOP

CrawlerSQLIXSSSSHintruder



AssassinGo

Home

Recon

Attack

Assassinate

Seek

Seek

seek

cyber security

30

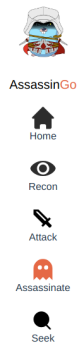
SEARCH

Domain Treatment ☒

#	URL
401	https://www.mozilla.org/
402	http://www.northropgrumman.com/
403	https://www.century.edu/
404	http://www.api.org/
405	https://www.itu.int/
406	http://www.sjsu.edu/
407	http://www.cybersecurityacademy.com/
408	http://www.longwood.edu/

Seek

4



Assassinate

drupal-rce

amyang.xyz

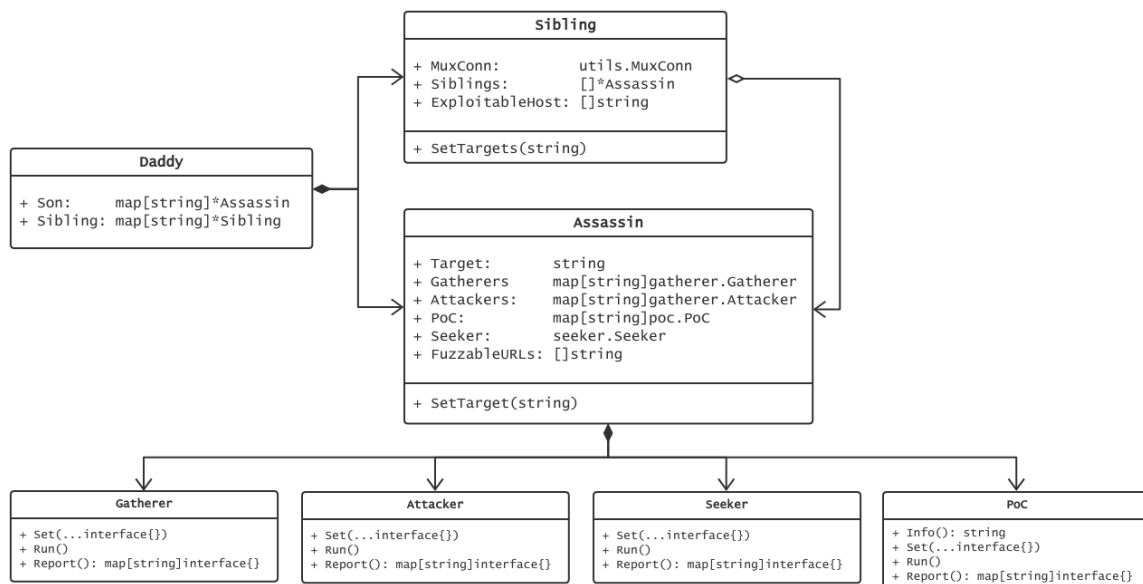
ATTACK

POC INFO		#	URL	STATUS
Date	2018-04-25	1	amyang.xyz	false
ID	CVE-2018-7602			
Platform	PHP			
Reference	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7602			
Text	biubiubiu			
Type	Remote Code Execution			

Poc

Outline Design

I choose **Composite Pattern** to increase expansibility.



API

AJAX

Path	Method	Func	Params	Return
/token	POST	sign in	username=admin&password=1234567890	{SSWToken:eyJhbGciOiJIUzI1NiIsInR5cGEiOiJ1d2UiLCJ0eXciOiJ0cm9udCIsImVudCI6IjE5OTY5MjE0IiwiaWF0IjoiMTU5OTY5MjE0In0= (stored in cookie)}
/api/target	POST	set a target	target=xxx OR targets=t1,t2...	nil
/api/info/basic	GET	get ip and retrieve security headers	nil	{data:{“ip”: “192.168.1.1”, “webserver”: “nginx”, “click_jacking_protection”:true}}
/api/info/bypasscf	GET	find real ip behind cloudflare	nil	{“real_ip”:“123.123.123.123”}
/api/info/cms	GET	detect cms	nil	{data:{“cms”: “wordpress”}}
/api/info/honeypot	GET	get ip and webserver	nil	{data:{“score”: “0.3”}}
/api/info/whois	GET	whois	nil	{data:{“domain”:“example.com”, “ad-min_name”:“xiaoming”, “ad-min_email”:“a@qq.com”, “ad-min_phone”:“+86.12312345678”, “created_date”:“2016-07-28T12:57:53.OZ”, “expiration_date”:“2017-07-28T12:57:53.OZ”, “ns”:“dns9.hichina.com”, “state”:“clienttransferprohibited”}}

Path	Method	Func	Params	Return
/api/poc	GET	get poc list	nil	{data:{“poc_list”:[“drupal-rce”:{“id”：“CVE-2017-7602”,“type”：“remote code execution”,“text”：“biubiubiu”,“platform”：“linux”,“date”：“2017-04-25”,##“reference”：“https://cve.mitre.org/cve/2017/7602”,“bin/cvename.cgi?name=CVE-2018-7602”},“seacms-v654-rce”]}##}}
/api/poc/:poc	GET	run the specified poc	nil	{data:{“host”：“example.com”,“exploitable”：“true”}}

WebSocket

Path	Func	Params	Return
/ws/info/port	port scan	nil	{“port”: “80”, “service”: “http”}
/ws/info/tracert	trace route and mark on google map	nil	{“ttl”: 1, “addr”: 192.168.1.1, “elapsed_time”: 22720440, “country”: China, “lat”: 34.2583, “long”: 116.1614}
/ws/info/subdomain	enum subdomain	nil	{“subdomain”：“earth.google.com”}

Path	Func	Params	Return
/ws/info/dirb	brute force dir	{“concurrency”:20, “dict”:“php”}; {“stop”:1}	{“path”: “admin.php”, “resp_status”: 200, “resp_len”: 110}
/ws/attack/crawl	crawl paramed urls	{“max_depth”: 4}	{“url”: “example.com/?id=1”}
/ws/attack/sqli	check sqli	nil	{“sqli_url”: “example.com/?id=1”}
/ws/attack/xss	check xss	nil	{“xss_url”: “example.com/?id=1”}
/ws/attack/intrude	brute force	{“header”: “GET / HTTP/1.1 ...”, “payload”: “p1,p2...”, “concurrency”: “10”}; {“stop”:1}	{“payload”: 1, “resp_status”: 200, “resp_len”: 110}
/ws/attack/ssh	brute force ssh	{“port”:“22”, “concurrency”:40}	{“user”:“root”,“passwd”:“biubiubiu”}
/ws/seek	seek targets	{“query”: “biu”, “se”: “bing/google”, “max_page”: 10}	{“urls”: urls}
/ws/poc/:poc	run poc	{concurrency:10}	{“exploitable_host”: “example.com”}

License

MIT