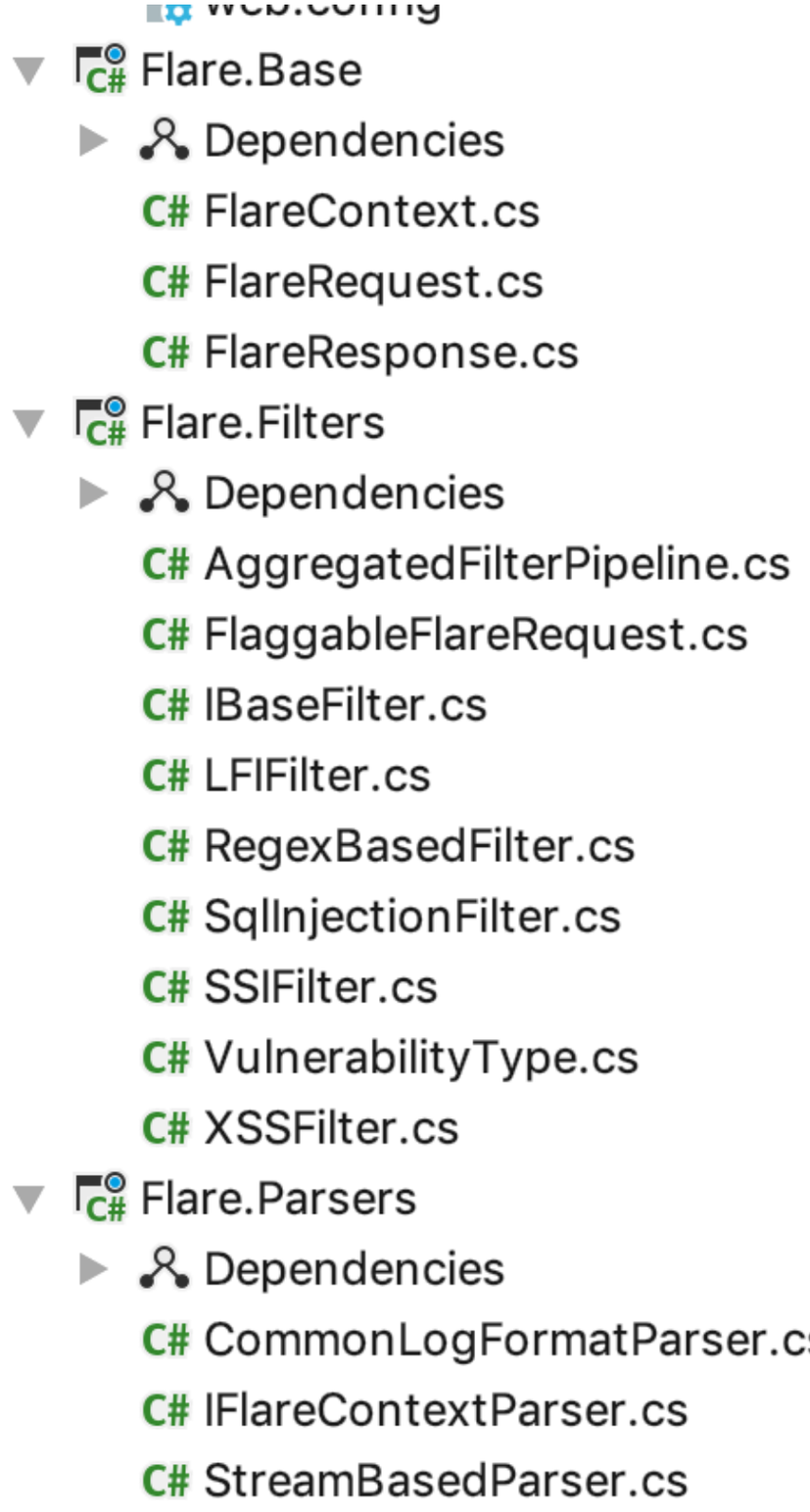
takeover.c team

Flare - Web Application Firewall

Alexander Badrishvili & Burak Tamturk

Technologies

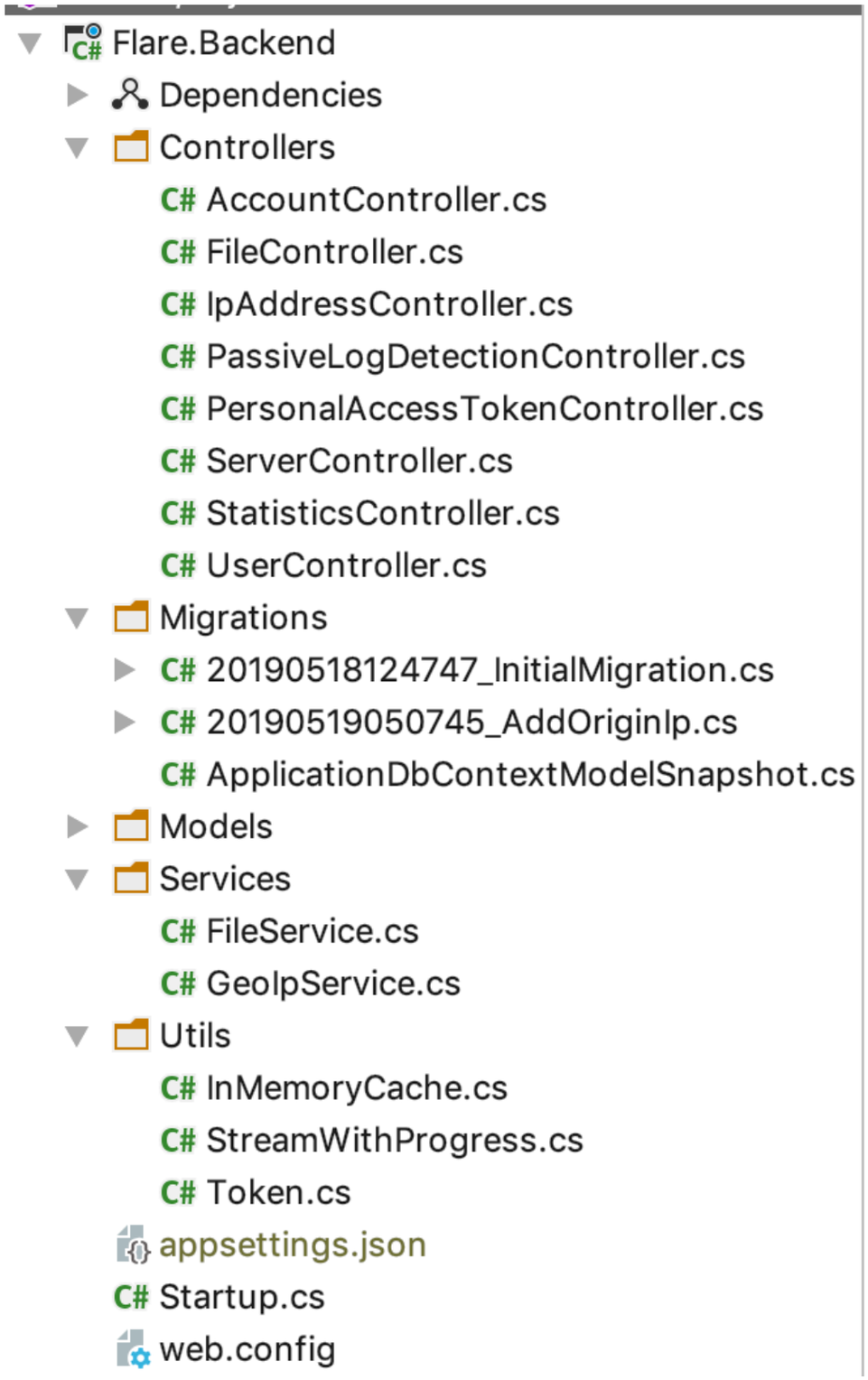
- Backend: C#, ASP.NET Core, MVC, Entity Framework Core with Code First and MySQL. REST / JSON API endpoint.
- Frontend: WebPack, AngularJS and Google Charts.
- Production: 2 Linux servers (1 db, 1 web), Nginx web server backing the .NET application.
- Let’sEncrypt



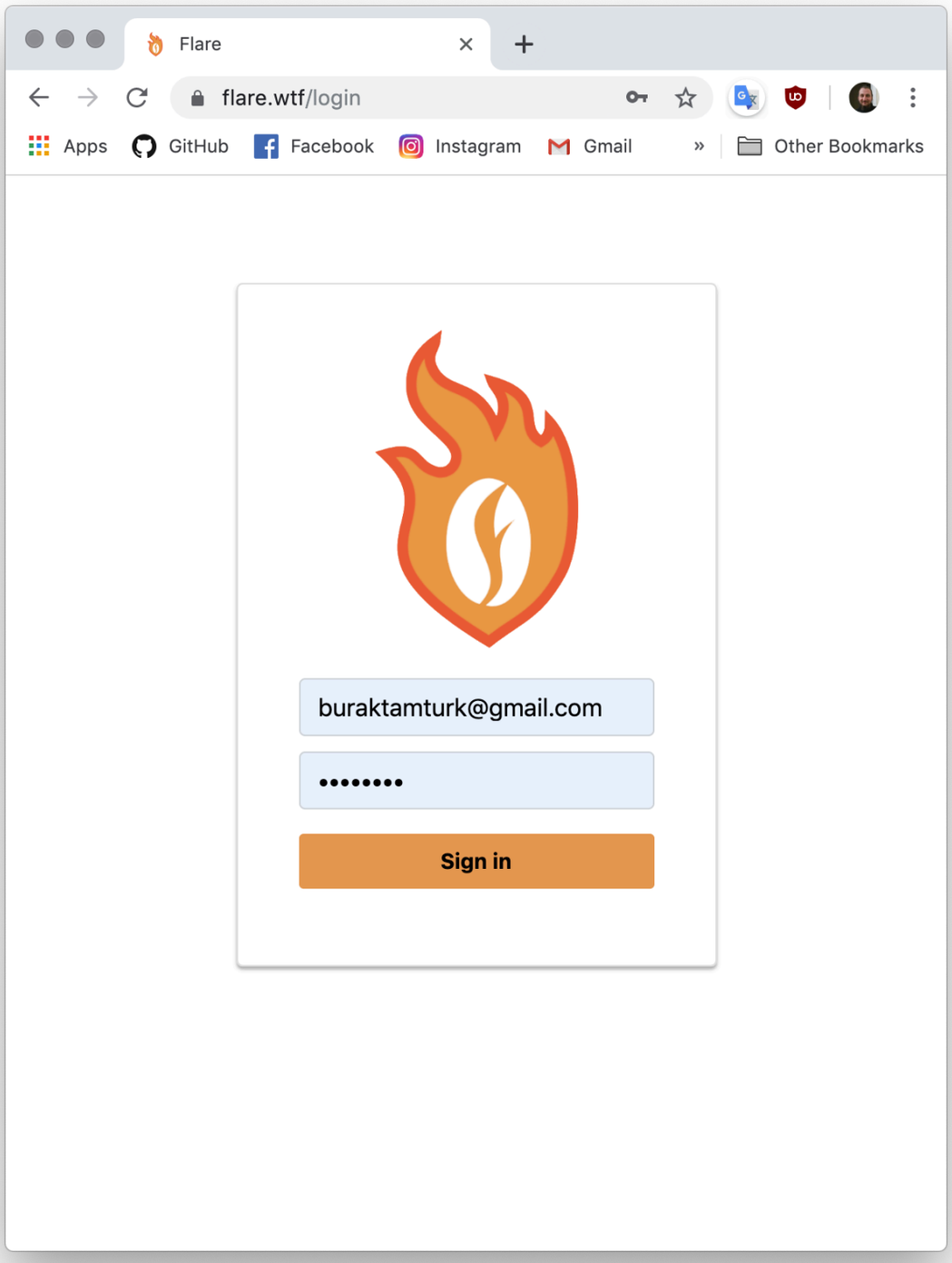
- FlareContext: Common response/ request models.

- IBaseFilter: Provides pipeline for various attack techniques.

- IFlareContextParser: Interface that is implemented by StreamBasedParser (file logs) and CLRParser (apache2 logs)



- Server Application: oauth2, JWT tokens, MaxMind GeoIP and separated containers for websites.



- Frontend: published on https://flare.wtf/
- This is login page.
- Default credentials: buraktamturk@gmail.com 123456

Flare

flare.wtf

Apps GitHub Facebook Instagram Gmail Hacker News Tureng » Other Bookmarks

Burak Tamturk Logout

Servers

Users

Tokens

Flare

flare.wtf/user

Apps GitHub Facebook Instagram Gmail Hacker News Tureng Phoronix ekşi sözlük 9GAG » Other Bookmarks

Burak Tamturk Logout

Home / Users

+ Add User Search...

ID	Avatar	Name	Type	E-Mail	Created at	Actions
1		Burak Tamturk	Admin	buraktamturk@gmail.com	Jan 1, 1 1:34:52 AM	Edit Delete

Avatar:

Upload Image

Name:

Burak Tamturk

E-Mail:

buraktamturk@gmail.com

Type:

Admin

Password:

••••••••

Save

Cancel

Servers page

Flare

Burak Tamturk Logout

Home / Servers

+ Add Server

ID	Name	Created at	Actions
2	Greek NGO	May 19, 2019 11:39:52 AM	Edit Upload Log Analysis Delete
3	Alex's Server Demo	May 19, 2019 11:51:19 AM	Edit Upload Log Analysis Delete

Name:

Alex's Server Demo

Enable cloud based protection

Block malicious requests

Origin IP:

193.70.76.107

Domains:

demo.badrishvili.com

Type here to add new...

Delete existing **A** or **CNAME** records from these domains and put **CNAME** record with a value of **cnd.flare.wtf**

For extended security, only allow connections from **176.31.106.179** where we filter the requests and proxy to your server.

Save

Cancel

Name:

Greek NGO

Enable cloud based protection

Save

Cancel

```
220.243.135.5 - - [18/May/2019:00:00:00 +0200] "GET /api/v1/login/?username=admin&password=1234 HTTP/1.1" 200 16981
62.109.16.162 - - [18/May/2019:00:00:01 +0200] "GET /login.php/?id=0%20or%201=1 HTTP/1.0" 404 53109
87.251.81.179 - - [18/May/2019:00:00:02 +0200] "GET /core/files/js/editor.js/.well-known/assetlinks.json HTTP/1.0" 200 84
182.34.27.162 - - [18/May/2019:00:00:03 +0200] "GET /index.php/ HTTP/1.0" 200 30803
182.34.27.162 - - [18/May/2019:00:00:03 +0200] "GET /index.php/ HTTP/1.0" 200 78913
182.34.27.162 - - [18/May/2019:00:00:03 +0200] "GET /index.php/ HTTP/1.0" 200 3547
182.34.27.162 - - [18/May/2019:00:00:03 +0200] "GET /index.php/ HTTP/1.0" 200 68064
182.34.27.162 - - [18/May/2019:00:00:03 +0200] "GET /index.php/ HTTP/1.0" 200 88626
220.243.135.5 - - [18/May/2019:00:00:08 +0200] "GET /index.php/?username=admin&password=1238 HTTP/1.0" 200 44700
121.225.26.201 - - [18/May/2019:00:00:09 +0200] "GET /api/v1/login/?customerId=1OR%201=1 HTTP/1.0" 200 70306
115.221.121.44 - - [18/May/2019:00:00:10 +0200] "POST /api/v1/customers/\xf5@~\xcc\r\xfdKJ\x0c=u[c\xfb+3\x88\xd2%z HTTP/1
183.87.255.54 - - [18/May/2019:00:00:11 +0200] "GET /api/v1/login/?username=admin&password=1236 HTTP/1.1" 404 89289
115.221.121.44 - - [18/May/2019:00:00:12 +0200] "POST /index.php/ HTTP/1.0" 200 70738
115.221.121.44 - - [18/May/2019:00:00:13 +0200] "GET /update.php/?username=admin&password=1236 HTTP/1.1" 200 11961
75.140.82.208 - - [18/May/2019:00:00:14 +0200] "POST /index.php/ HTTP/1.0" 404 49118
75.140.82.208 - - [18/May/2019:00:00:14 +0200] "POST /index.php/ HTTP/1.0" 404 84171
75.140.82.208 - - [18/May/2019:00:00:14 +0200] "POST /index.php/ HTTP/1.0" 404 61029
75.140.82.208 - - [18/May/2019:00:00:14 +0200] "POST /index.php/ HTTP/1.0" 404 55926
```

- On 18 May and later - the Greek timezone is +0300. Log file has invalid timestamps or times that does not fit in a single day. We manually fixed it by doing search and replace.

ID	Name	Created at	Actions
2	Greek NGO	May 19, 2019 11:39:52 AM	Edit Upload Log Analysis Delete
3	Alex's Server Demo	May 19, 2019 11:51:19 AM	Edit Upload Log Analysis
5			

Processing the data: 13.869536288172124%

Burak Tamturk Logout

General

1. How much traffic has the server handled?

It handled **86400** requests resulting **3.6 GB** of response data from **May 18, 2019 12:00:00 AM** to **11:59:59 PM**.

2. How many requests generated requests a 5xx server error?

4729 requests returned 5xx server error.

3. How many distinct IPs visited the server?

20 distinct IP addresses have visited the server.

Data Mining

1. What percentage of the requests do you consider a server attack?

45.56%

2. How many SQL Injections, XSS and "Local File Inclusion (LFI)" attacks have you recognised in total?

39364 attacks in total divided by following:

1. **SQL Injection**: **8463** attacks. **21.50%** of total attacks.
2. **XSS (Cross-Site Scripting)**: **18796** attacks. **47.75%** of total attacks.
3. **LFI (Local File Inclusion)**: **1203** attacks. **3.06%** of total attacks.
4. **SSI (Server Side Injection)**: **10902** attacks. **27.70%** of total attacks.

3. Which 5 pages had the most attacks?

1. **/**: **6976** attacks. **17.72%** of total attacks.
2. **/index.php/**: **5651** attacks. **14.36%** of total attacks.
3. **/login.php/**: **4188** attacks. **10.64%** of total attacks.
4. **/api/v1/login/**: **2905** attacks. **7.38%** of total attacks.
5. **/core/files/js/upload.js/**: **2105** attacks. **5.35%** of total attacks.

4. Which country generated the most attacks?

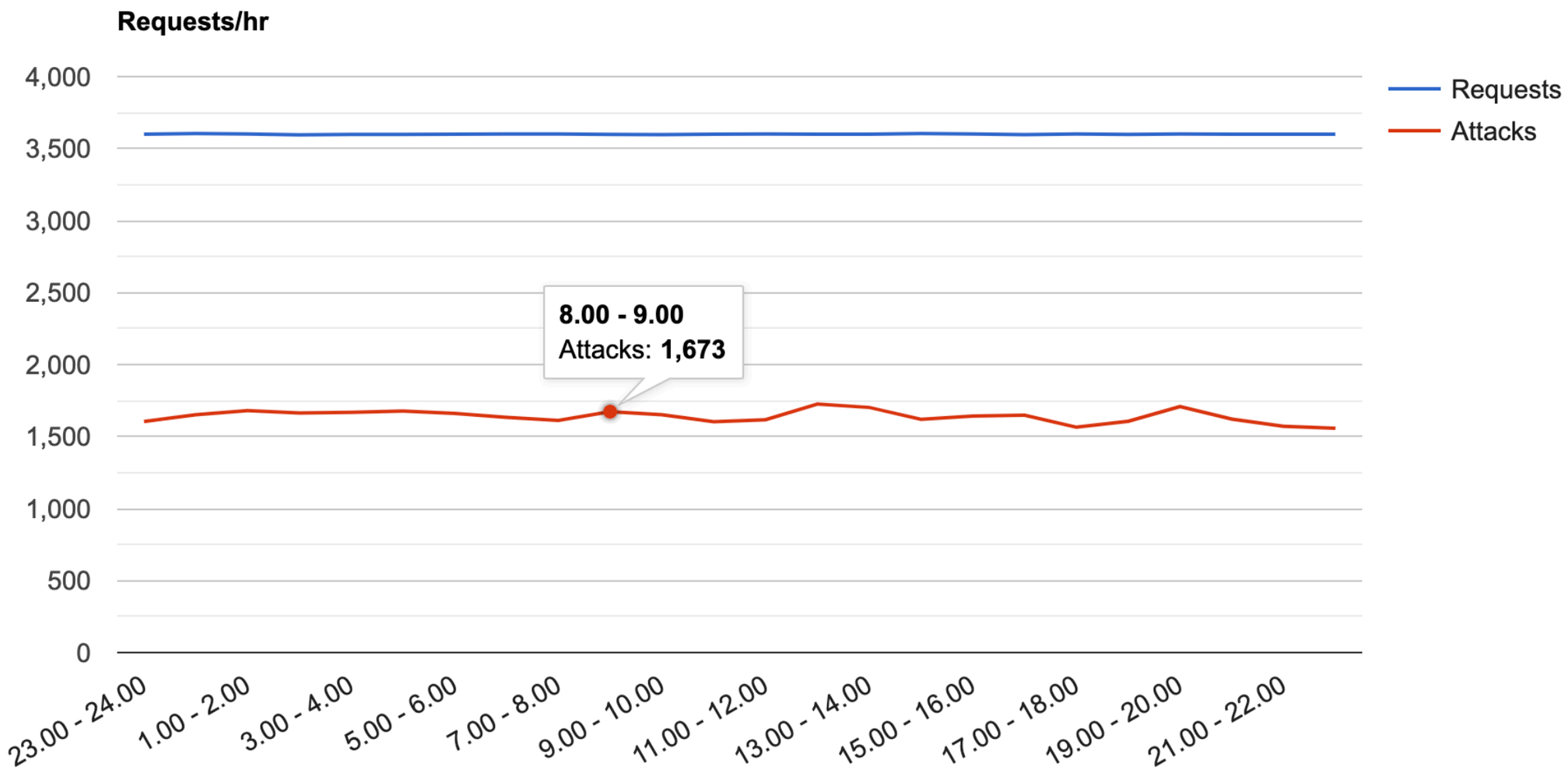
1. **China**: **13655** attacks. **34.69%** of total attacks.
2. **Russia**: **12744** attacks. **32.37%** of total attacks.
3. **United States**: **4472** attacks. **11.36%** of total attacks.
4. **India**: **2554** attacks. **6.49%** of total attacks.
5. **France**: **2413** attacks. **6.13%** of total attacks.
6. **Romania**: **1293** attacks. **3.28%** of total attacks.
7. **Pakistan**: **1014** attacks. **2.58%** of total attacks.
8. **Thailand**: **624** attacks. **1.59%** of total attacks.
9. **Greece**: **595** attacks. **1.51%** of total attacks.

5. What time of the day generated the most attacks?

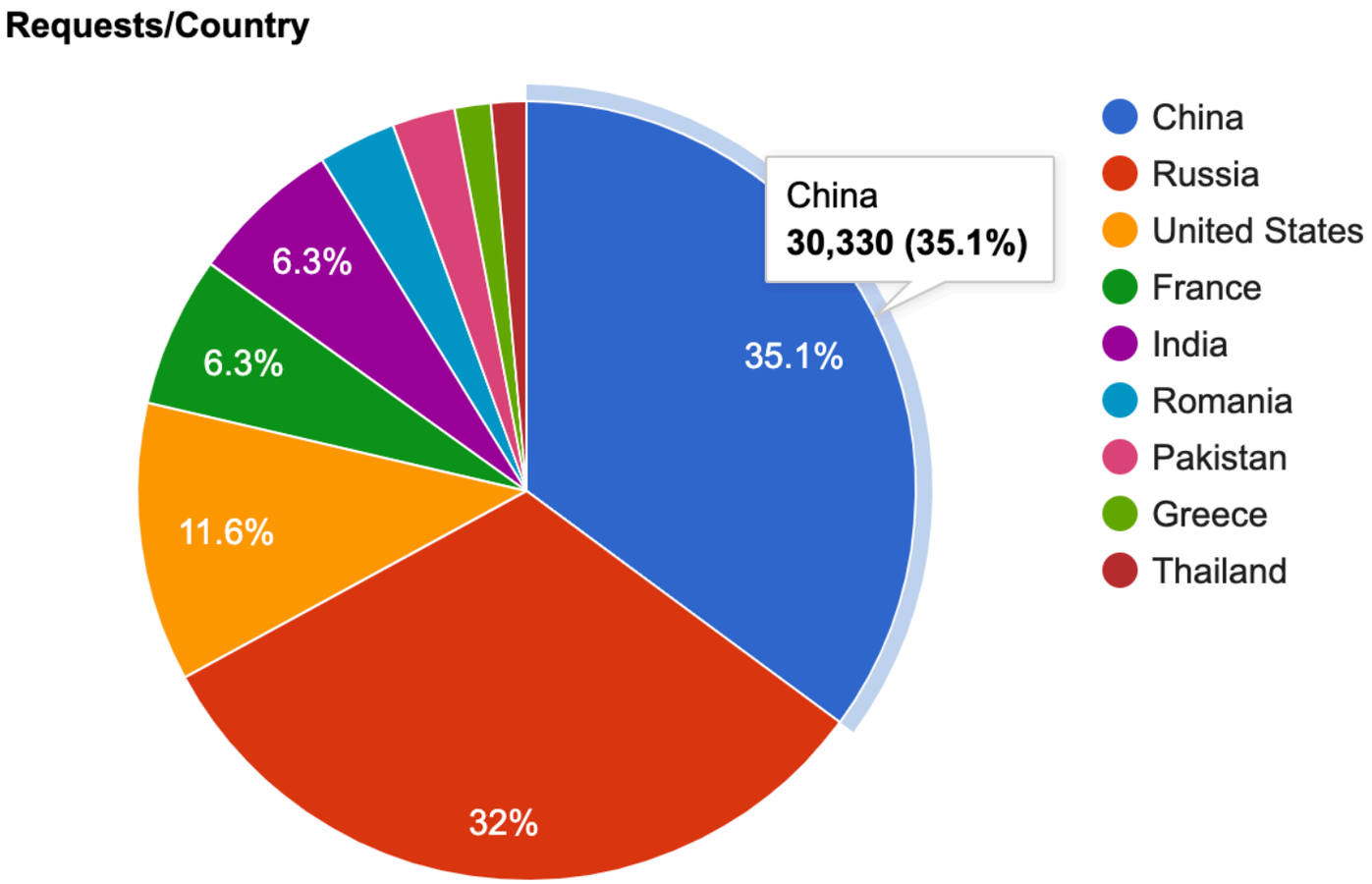
1. **12.00 - 13.00**: **1725** attacks. **4.38%** of total attacks.
2. **19.00 - 20.00**: **1709** attacks. **4.34%** of total attacks.
3. **13.00 - 14.00**: **1702** attacks. **4.32%** of total attacks.
4. **1.00 - 2.00**: **1681** attacks. **4.27%** of total attacks.
5. **4.00 - 5.00**: **1678** attacks. **4.26%** of total attacks.

UI - Visualisation

1. Visualise the number of server requests/hr in a graph (Requests per Hour)



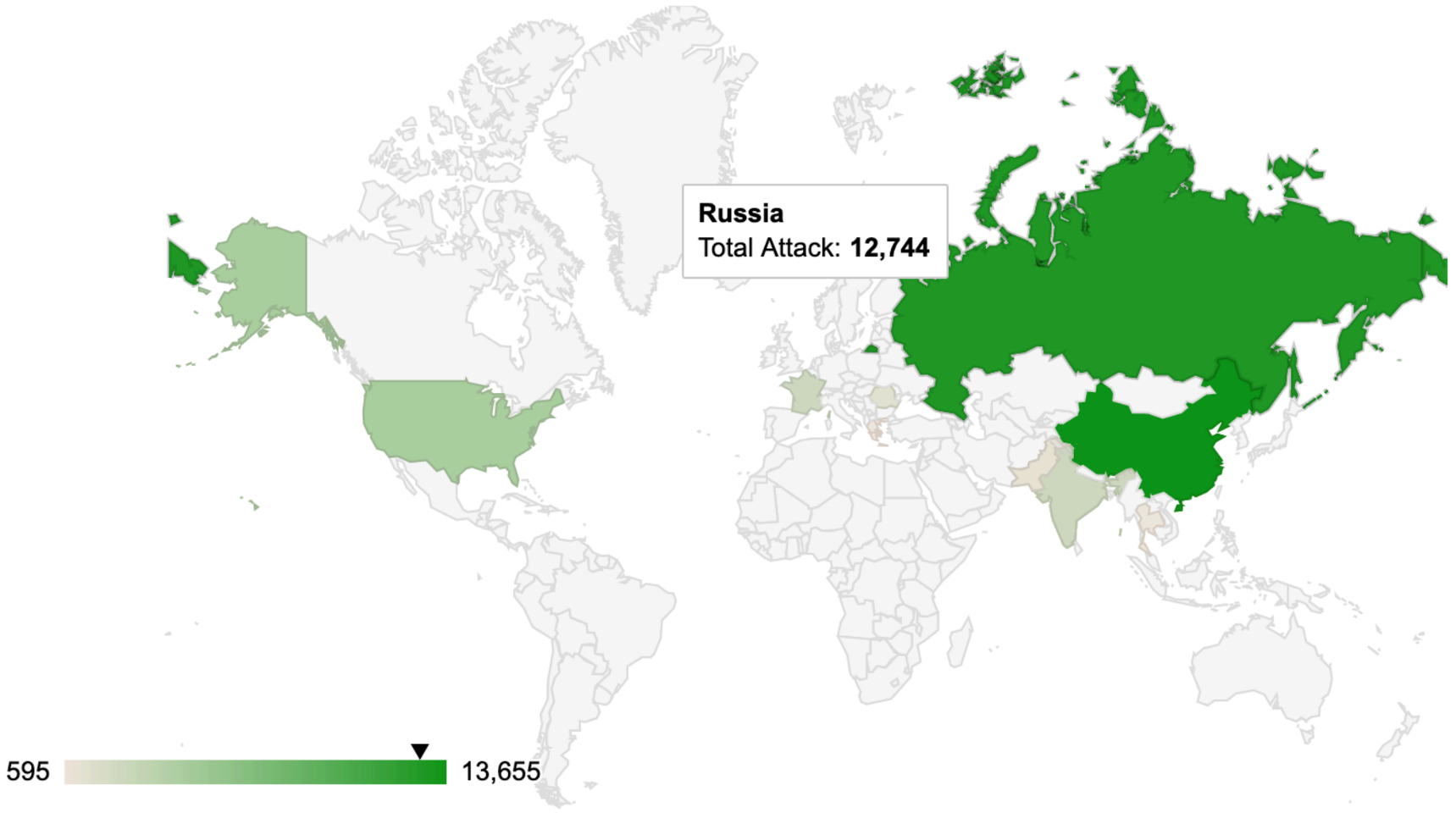
2. Visualise the total number of server requests/country in a pie chart (Total Requests per Country)



3. Visualise the attack requests/hour on a map

Filter by hour

Select Hour...

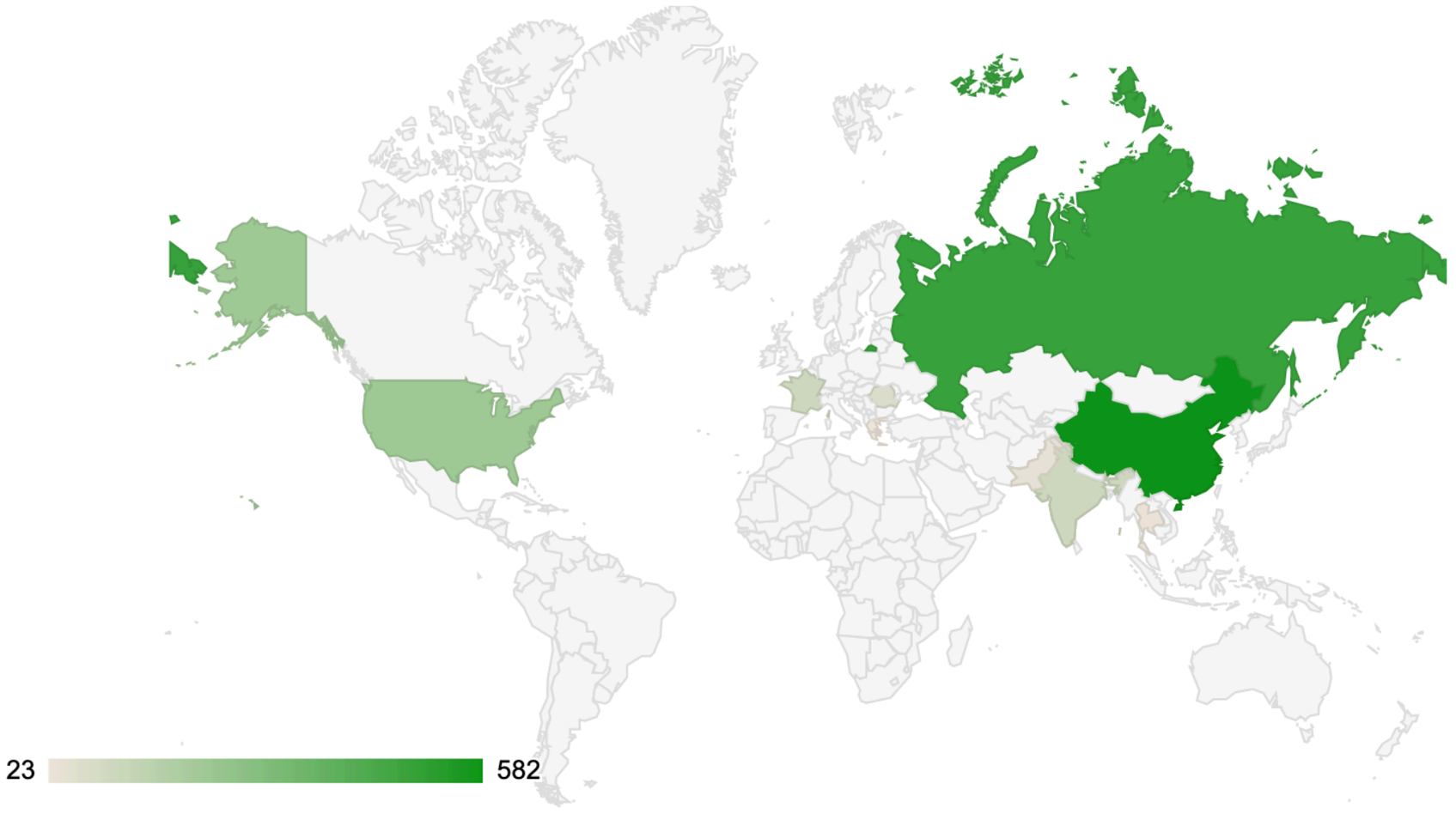


3. Visualise the attack requests/hour on a map

Filter by hour

15.00 - 16.00

Clear selection



Stats for Nerds

Bonus

1. ### Which is the most dangerous IP according to you and why?

   It is **87.251.81.179** and originates from **Russia**. It made **5.94%** of total attacks (that is **5135** attacks) among of **4** vulnerabilities that is **1.42%** more compared to its international rival (**121.225.26.201** / **China**) . This IP seems belong to "**OOO Network of data-centers Selectel**" and it looks like it is **residental** network and city information not available for this specific IP address but we have **62.109.16.162** which **is also** originates from **Russia**. Although it made **-0.09%** less attacks. We know it is located in the city of **Tula** of **Russia** .

The changing answer depending on the data

Bonus

1. **Which is the most dangerous IP according to you and why?**

   It is **83.212.59.173** and originates from **Greece**. It made **60.00%** of total attacks (that is **6** attacks) among of **2** vulnerabilities that is **50.00%** more compared to its international rival (**8.8.8.8** / **United States**) . This IP seems belong to "**Network of TEI Serres**" , ISP providing this IP is "**Greek Research and Technology Network S.A**" and the city this IP belongs to **Serres**.

General

1. How much traffic has the server handled?

It handled **13** requests resulting **115.5 kB** of response data from **May 19, 2019 11:51:34 AM** to **1:52:19 PM**.

2. How many requests generated requests a 5xx server error?

0 requests returned 5xx server error.

3. How many distinct IPs visited the server?

2 distinct IP addresses have visited the server.

Data Mining

1. What percentage of the requests do you consider a server attack?

61.54%

2. How many SQL Injections, XSS and "Local File Inclusion (LFI)" attacks have you recognised in total?

8 attacks in total divided by following:

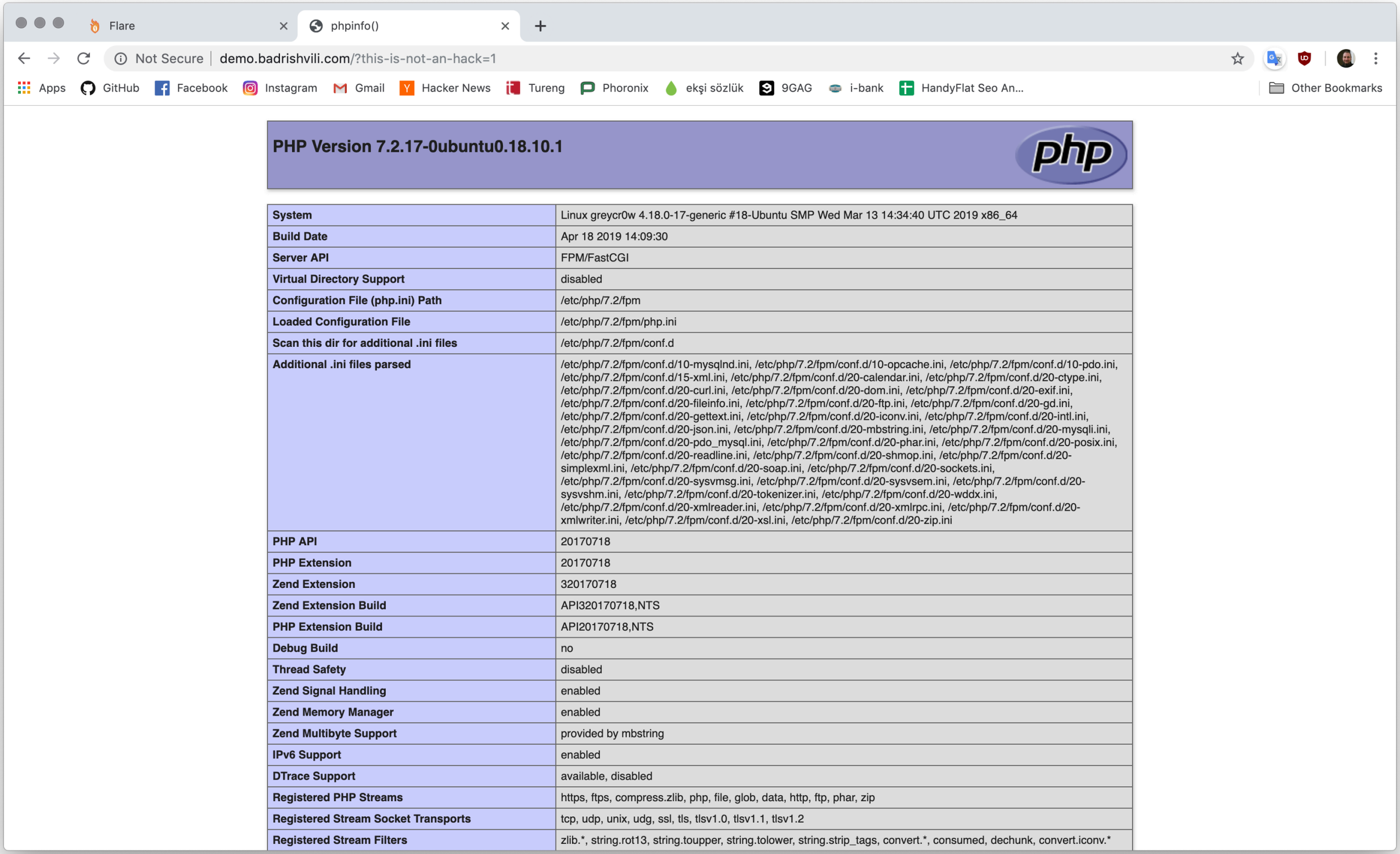
1. **SQL Injection**: **7** attacks. **87.50%** of total attacks.
2. **XSS (Cross-Site Scripting)**: **1** attacks. **12.50%** of total attacks.

3. Which 5 pages had the most attacks?

1. **/**: **8** attacks. **100.00%** of total attacks.

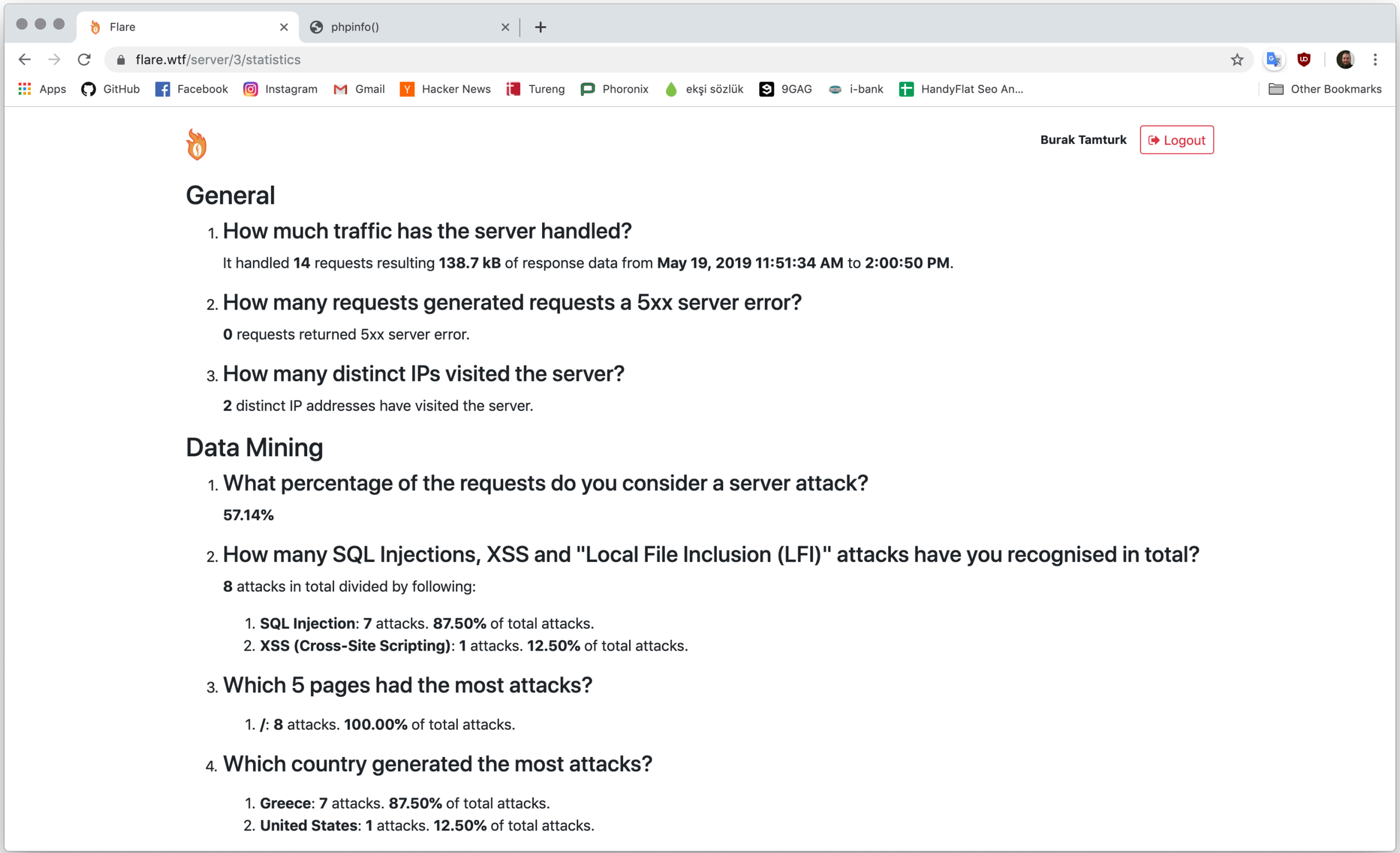
4. Which country generated the most attacks?

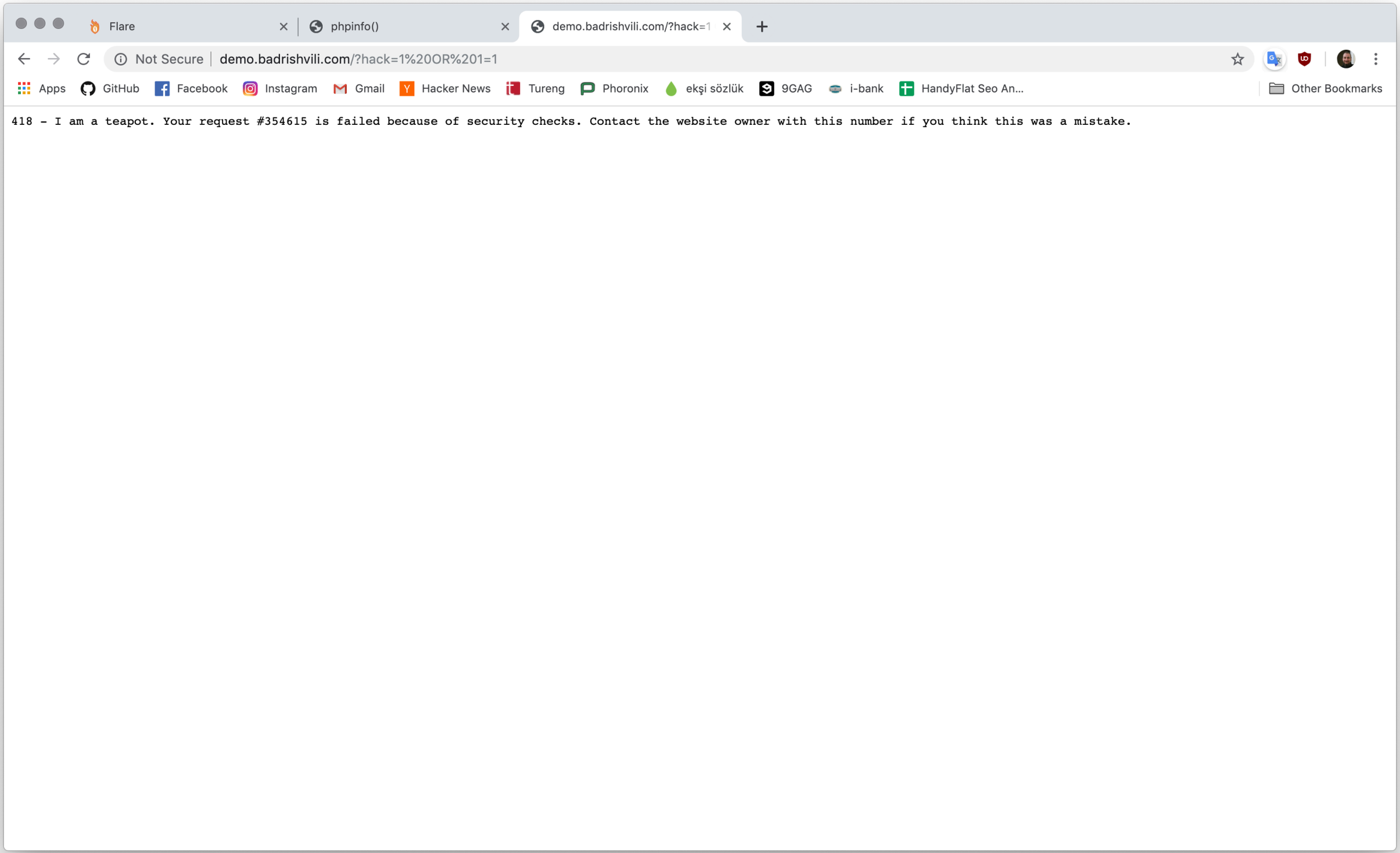
1. **Greece**: **7** attacks. **87.50%** of total attacks.
2. **United States**: **1** attacks. **12.50%** of total attacks.



PHP Version 7.2.17-0ubuntu0.18.10.1

System	Linux greycr0w 4.18.0-17-generic #18-Ubuntu SMP Wed Mar 13 14:34:40 UTC 2019 x86_64
Build Date	Apr 18 2019 14:09:30
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/fpm
Loaded Configuration File	/etc/php/7.2/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/7.2/fpm/conf.d
Additional .ini files parsed	/etc/php/7.2/fpm/conf.d/10-mysqlnd.ini, /etc/php/7.2/fpm/conf.d/10-opcache.ini, /etc/php/7.2/fpm/conf.d/10-pdo.ini, /etc/php/7.2/fpm/conf.d/15-xml.ini, /etc/php/7.2/fpm/conf.d/20-calendar.ini, /etc/php/7.2/fpm/conf.d/20-ctype.ini, /etc/php/7.2/fpm/conf.d/20-curl.ini, /etc/php/7.2/fpm/conf.d/20-dom.ini, /etc/php/7.2/fpm/conf.d/20-exif.ini, /etc/php/7.2/fpm/conf.d/20-fileinfo.ini, /etc/php/7.2/fpm/conf.d/20-ftp.ini, /etc/php/7.2/fpm/conf.d/20-gd.ini, /etc/php/7.2/fpm/conf.d/20-gettext.ini, /etc/php/7.2/fpm/conf.d/20-iconv.ini, /etc/php/7.2/fpm/conf.d/20-intl.ini, /etc/php/7.2/fpm/conf.d/20-json.ini, /etc/php/7.2/fpm/conf.d/20-mbstring.ini, /etc/php/7.2/fpm/conf.d/20-mysqli.ini, /etc/php/7.2/fpm/conf.d/20-pdo_mysql.ini, /etc/php/7.2/fpm/conf.d/20-phar.ini, /etc/php/7.2/fpm/conf.d/20-posix.ini, /etc/php/7.2/fpm/conf.d/20-readline.ini, /etc/php/7.2/fpm/conf.d/20-shmop.ini, /etc/php/7.2/fpm/conf.d/20-simplexml.ini, /etc/php/7.2/fpm/conf.d/20-soap.ini, /etc/php/7.2/fpm/conf.d/20-sockets.ini, /etc/php/7.2/fpm/conf.d/20-sysvmsg.ini, /etc/php/7.2/fpm/conf.d/20-sysvsem.ini, /etc/php/7.2/fpm/conf.d/20-sysvshm.ini, /etc/php/7.2/fpm/conf.d/20-tokenizer.ini, /etc/php/7.2/fpm/conf.d/20-wddx.ini, /etc/php/7.2/fpm/conf.d/20-xmlreader.ini, /etc/php/7.2/fpm/conf.d/20-xmlrpc.ini, /etc/php/7.2/fpm/conf.d/20-xmlwriter.ini, /etc/php/7.2/fpm/conf.d/20-xsl.ini, /etc/php/7.2/fpm/conf.d/20-zip.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,NTS
PHP Extension Build	API20170718,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*


Flare
phpinfo()
flare.wtf/server/3/statistics
Apps
GitHub
Facebook
Instagram
Gmail
Hacker News
Tureng
Phoronix
ekşi sözlük
9GAG
i-bank
HandyFlat Seo An...
Other Bookmarks
Burak Tamturk
Logout
General
1. How much traffic has the server handled?
It handled 14 requests resulting 138.7 kB of response data from May 19, 2019 11:51:34 AM to 2:00:50 PM.
2. How many requests generated requests a 5xx server error?
0 requests returned 5xx server error.
3. How many distinct IPs visited the server?
2 distinct IP addresses have visited the server.
Data Mining
1. What percentage of the requests do you consider a server attack?
57.14%
2. How many SQL Injections, XSS and "Local File Inclusion (LFI)" attacks have you recognised in total?
8 attacks in total divided by following:
1. SQL Injection: 7 attacks. 87.50% of total attacks.
2. XSS (Cross-Site Scripting): 1 attacks. 12.50% of total attacks.
3. Which 5 pages had the most attacks?
1. /: 8 attacks. 100.00% of total attacks.
4. Which country generated the most attacks?
1. Greece: 7 attacks. 87.50% of total attacks.
2. United States: 1 attacks. 12.50% of total attacks.


Flare
phpinfo()
demo.badrishvili.com/?hack=1
Not Secure
demo.badrishvili.com/?hack=1%20OR%201=1
Apps
GitHub
Facebook
Instagram
Gmail
Hacker News
Tureng
Phoronix
ekşi sözlük
9GAG
i-bank
HandyFlat Seo An...
Other Bookmarks
418 - I am a teapot. Your request #354615 is failed because of security checks. Contact the website owner with this number if you think this was a mistake.

image/svg+xml, but the server requires that images use a different format.[48]

416 Range Not Satisfiable (RFC 7233)

The client has asked for a portion of the file (byte serving), but the server cannot supply that portion. For example, if the client asked for a part of the file that lies beyond the end of the file.[49] Called "Requested Range Not Satisfiable" previously.[50]

417 Expectation Failed

The server cannot meet the requirements of the Expect request-header field.[51]

418 I'm a teapot (RFC 2324, RFC 7168)

This code was defined in 1998 as one of the traditional IETF April Fools' jokes, in RFC 2324, *Hyper Text Coffee Pot Control Protocol*, and is not expected to be implemented by actual HTTP servers. The RFC specifies this code should be returned by teapots requested to brew coffee.[52] This HTTP status is used as an Easter egg in some websites, including Google.com.[53][54]

421 Misdirected Request (RFC 7540)

The request was directed at a server that is not able to produce a response[55] (for example because of connection reuse).[56]

422 Unprocessable Entity (WebDAV; RFC 4918)

The request was well-formed but was unable to be followed due to semantic errors.[17]

General

1. How much traffic has the server handled?

It handled **15** requests resulting **138.7 kB** of response data from **May 19, 2019 11:51:34 AM** to **2:01:56 PM**.

2. How many requests generated requests a 5xx server error?

0 requests returned 5xx server error.

3. How many distinct IPs visited the server?

2 distinct IP addresses have visited the server.

Data Mining

1. What percentage of the requests do you consider a server attack?

60.00%

2. How many SQL Injections, XSS and "Local File Inclusion (LFI)" attacks have you recognised in total?

9 attacks in total divided by following:

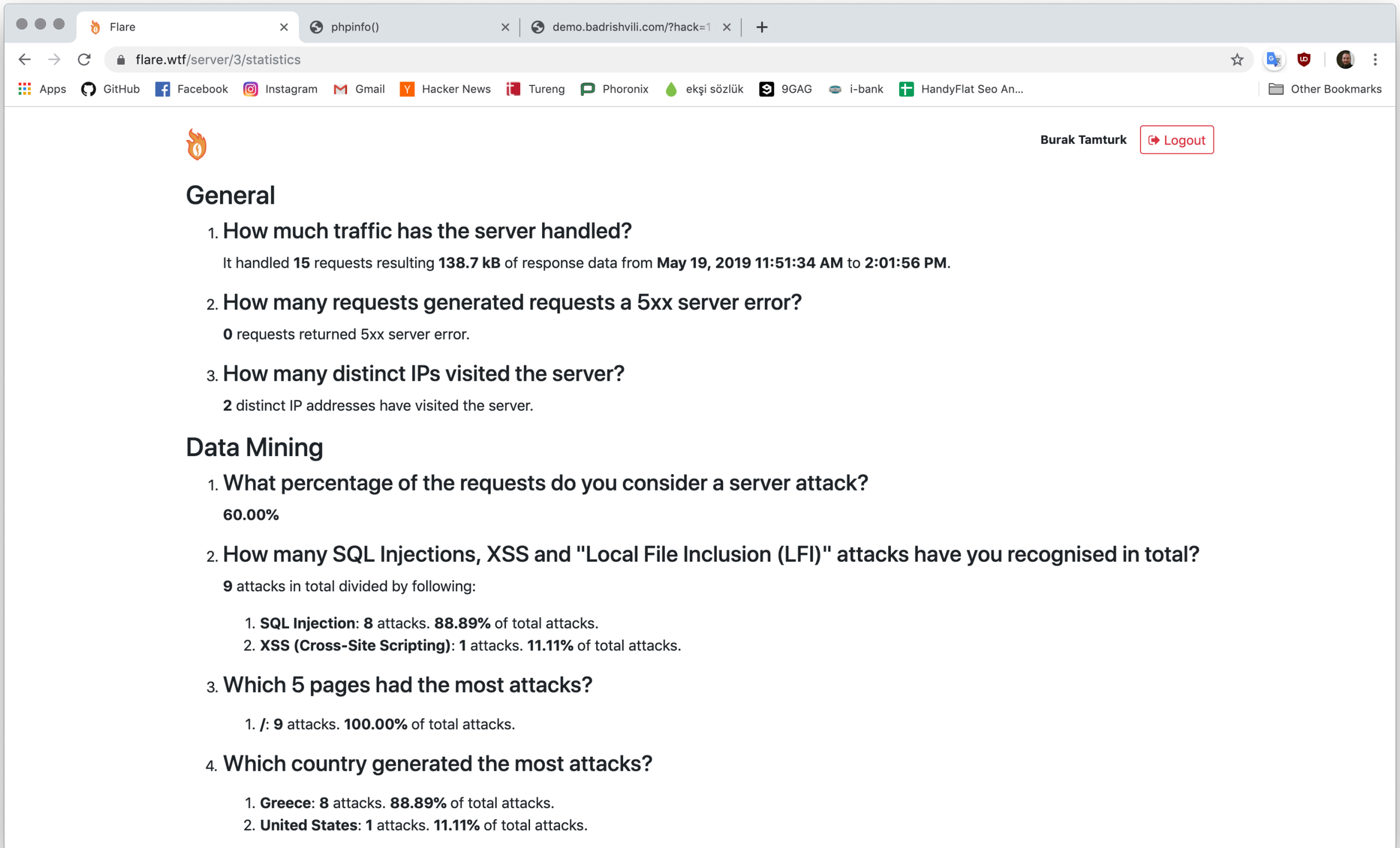
1. **SQL Injection**: **8** attacks. **88.89%** of total attacks.
2. **XSS (Cross-Site Scripting)**: **1** attacks. **11.11%** of total attacks.

3. Which 5 pages had the most attacks?

1. **/**: **9** attacks. **100.00%** of total attacks.

4. Which country generated the most attacks?

1. **Greece**: **8** attacks. **88.89%** of total attacks.
2. **United States**: **1** attacks. **11.11%** of total attacks.


Flare
phpinfo()
demo.badrishvili.com/?hack=1
flare.wtf/server/3/statistics
Apps
GitHub
Facebook
Instagram
Gmail
Hacker News
Tureng
Phoronix
ekşi sözlük
9GAG
i-bank
HandyFlat Seo An...
Other Bookmarks
Burak Tamturk
Logout
General
1. How much traffic has the server handled?
It handled 15 requests resulting 138.7 kB of response data from May 19, 2019 11:51:34 AM to 2:01:56 PM.
2. How many requests generated requests a 5xx server error?
0 requests returned 5xx server error.
3. How many distinct IPs visited the server?
2 distinct IP addresses have visited the server.
Data Mining
1. What percentage of the requests do you consider a server attack?
60.00%
2. How many SQL Injections, XSS and "Local File Inclusion (LFI)" attacks have you recognised in total?
9 attacks in total divided by following:
1. SQL Injection: 8 attacks. 88.89% of total attacks.
2. XSS (Cross-Site Scripting): 1 attacks. 11.11% of total attacks.
3. Which 5 pages had the most attacks?
1. /: 9 attacks. 100.00% of total attacks.
4. Which country generated the most attacks?
1. Greece: 8 attacks. 88.89% of total attacks.
2. United States: 1 attacks. 11.11% of total attacks.

Name:

Alex's Server Demo

Enable cloud based protection

Block malicious requests

Origin IP:

193.70.76.107

Domains:

demo.badrishvili.com

Type here to add new...

Delete existing **A** or **CNAME** records from these domains and put **CNAME** record with a value of **cnd.flare.wtf**

For extended security, only allow connections from **176.31.106.179** where we filter the requests and proxy to your server.

Save

Cancel

Burak Tamturk Logout

Home / Tokens

+ Add Token

ID	Label	Actions

Label:

My CLI Tool

Save

Cancel

Home / Tokens

+ Add Token

ID	Label	Created at	Last used	Actions
84629260-e7f5-4efd-a1ba-a4ed262				Edit Delete

Success!

username = 60926284F5E7FD4EA1BAA4ED2620F3B3
password = 3C20C9A59286C3928CDAA7A1B5A6335405BC40B

OK

curl --user CD3469F18FA30A48837BEE7FFB581107:D80082DBA1972012E507 --data-binary "log.1" https://api.flare.wtf/server/XXXX/apache2

Thank you!