BLIND XSS & FEMIDA

ZERO NIGHTS 2018

PAVEL RUKAVISHNIKOV
HD

ZERO NIGHTS 2018

2^3 EDITION

WHOAMI

PAVEL RUKAVISHNIKOV

- CTF PLAYER
- PROGRAMMER

GITHUB: HTTPS://GITHUB.COM/WISH-I-WAS
TWITTER: HTTPS://TWITTER.COM/WISH_IWAS

HD

- SCRIPT KIDDIE
- BOUNTY HUNTER
- PENTESTER

GITHUB: HTTPS://GITHUB.COM/HD421
TWITTER: HTTPS://TWITTER.COM/HD_421

2^3 EDITION

AGENDA

- WHAT IS BLIND XSS?
- HOW TO DEAL WITH IT
- WHERE TO INJECT
- CALLBACK HANDLERS
- HOW TO IMPROVE AND AUTOMATE
- TODO

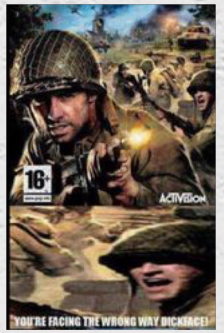
ZERO NIGHTS 2018

2^3 EDITION

FEW FACTS ABOUT BLIND XSS?

- ALMOST ALWAYS IT'S STORED
- YOU CAN'T SEE ALERT(1337)
- NEED YOUR PATIENCE

- FACING IT THE OTHER WAY



ZERO NIGHTS 2018

2^3 EDITION

WHERE TO INJECT

HEADERS:

- USER-AGENT
- REFERER
- ORIGIN
- X-FORWARDED-FOR

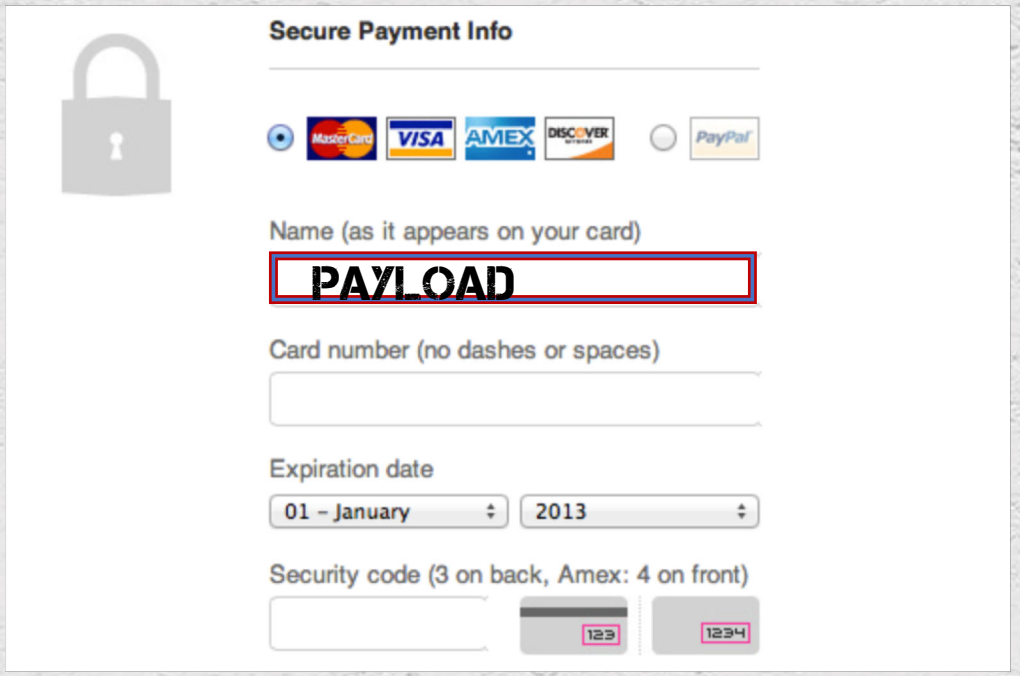
REQUEST PARAMETERS:

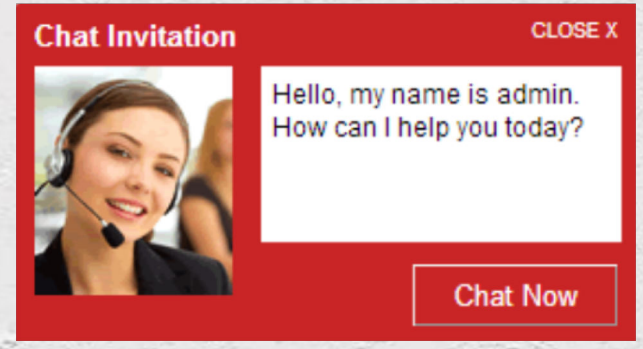
- IMAGINATION

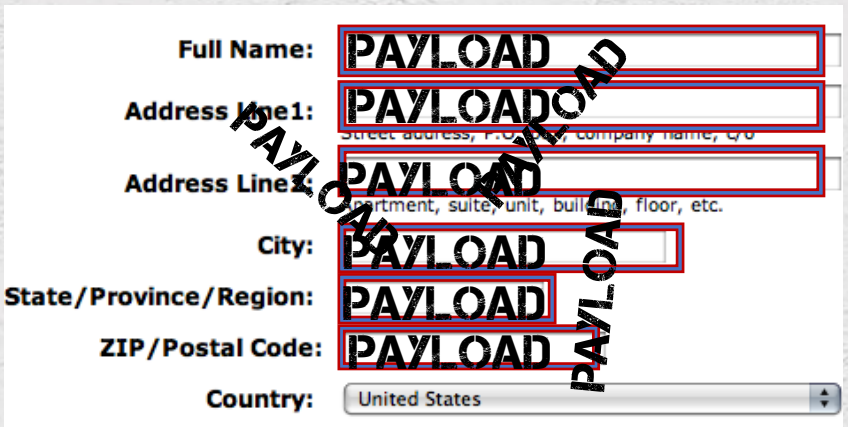
ZERO NIGHTS 2018

2³ EDITION

GROUND CONTROL







YOUR TARGET IS TO RECEIVE A KNOCK-KNOCK FROM APPLICATION USED BY ADMINISTRATOR/TEAM MEMBER

2018.ZERONIGHTS.ORG

2^3 EDITION

FEW MORE

Hello Super User,

We are sorry to find you are no longer interested in our newsletters.

- [x] Unsubscribe from this Mailing List
- [ ] Unsubscribe from all Mailing Lists
- [ ] Do not receive any e-mails from this website in the future

Before you go, we'd be grateful if you'd let us know why you're unsubscribing.

- [ ] The emails we send you are too frequent
- [ ] The emails we send are not relevant to you

Please add any other reasons here:

PAYLOAD

Unsubscribe

Contact us

Name

Email

Phone Number

PAYLOAD

Send

PASSWORD

••••••••••• PAYLOAD

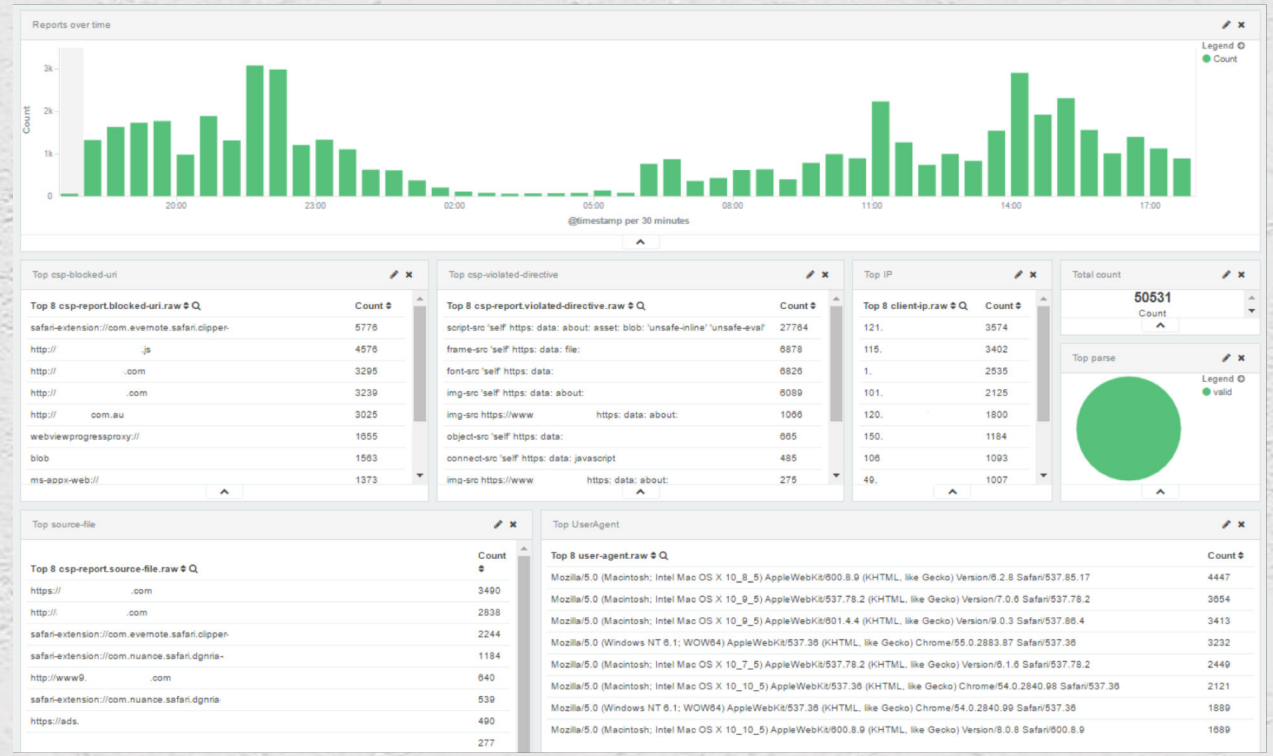
Great

2018.ZERONIGHTS.ORG

2^3 EDITION

CSP REPORT

- ALMOST ALWAYS REQUEST IS STATIC (EXCEPT CUSTOM CSP REPORTING FRAMEWORKS LIKE SENTRY CSP)
- PROCESSING SERVERS ARE OFTENLY POORLY PROTECTED



HOW IT LOOK SOMETIMES

2³ EDITION

SHOULD I LOOK FOR IT?

24 | zomato | **Blind XSS - Report review - Admin panel**
Zomato • by gerben_javado • $350 • Medium

14 | **[IMP] - Blind XSS in the admin panel for reviewing comments**
Rockstar Games • by anshuman_bh • $650 • Medium

47 | **Blind XSS in Mobpub Marketplace Admin Production | Sentry via demand.mopub.com (User-Agent)**
By harisec to Twitter | Resolved | High | $840

3 | **Stored Blind XSS**
By danila_xawdxawdx to Mail.Ru | Resolved | High | $500

ZERO NIGHTS 2018

2^3 EDITION

CALLBACK HANDLERS

ZERO NIGHTS 2018

2³ EDITION

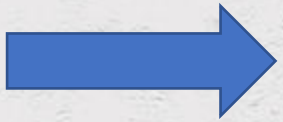
CALLBACK HANDLERS

2³ EDITION

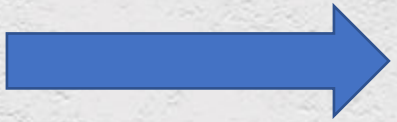
CALLBACK HANDLERS

https://github.com/jobertabma/ground-control

CALLBACK TOKEN



SSRF
XXE
XXS



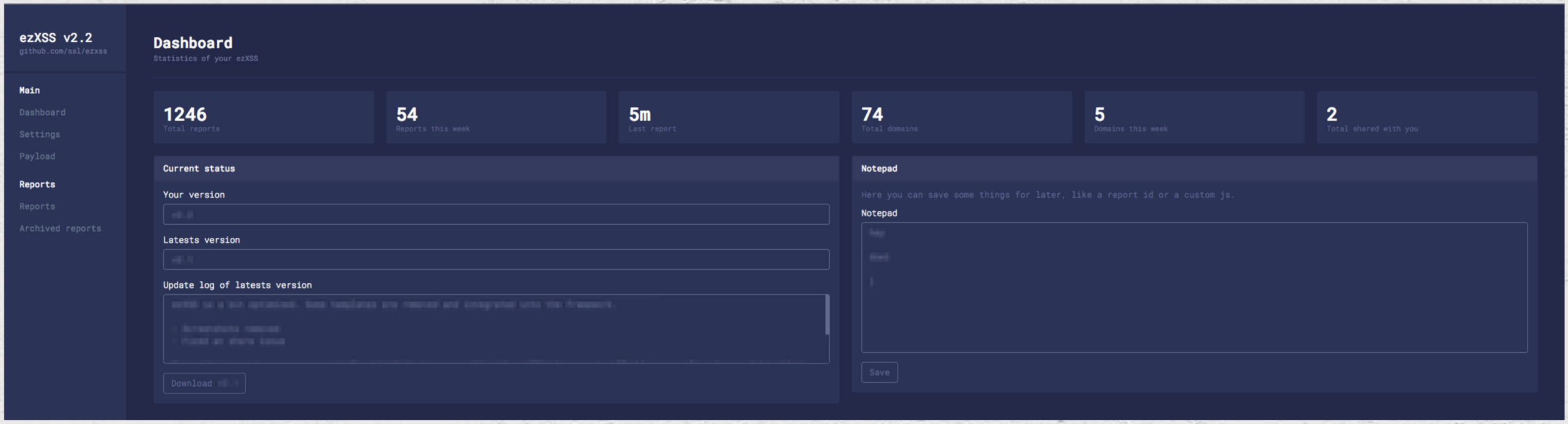
```
{
  "callback_tokens": {
    "ee34a1791ab345f789": {
      "host": "hackerone.com",
      "port": 443,
      "ssl": true,
      "path": "/webhooks",
      "parameter": "url",
      "method": "POST"
    }
  }
}
```

ZERO NIGHTS 2018

2^3 EDITION

CALLBACK HANDLERS

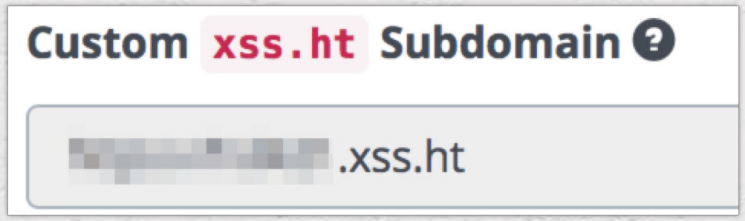
https://github.com/ssl/ezxss

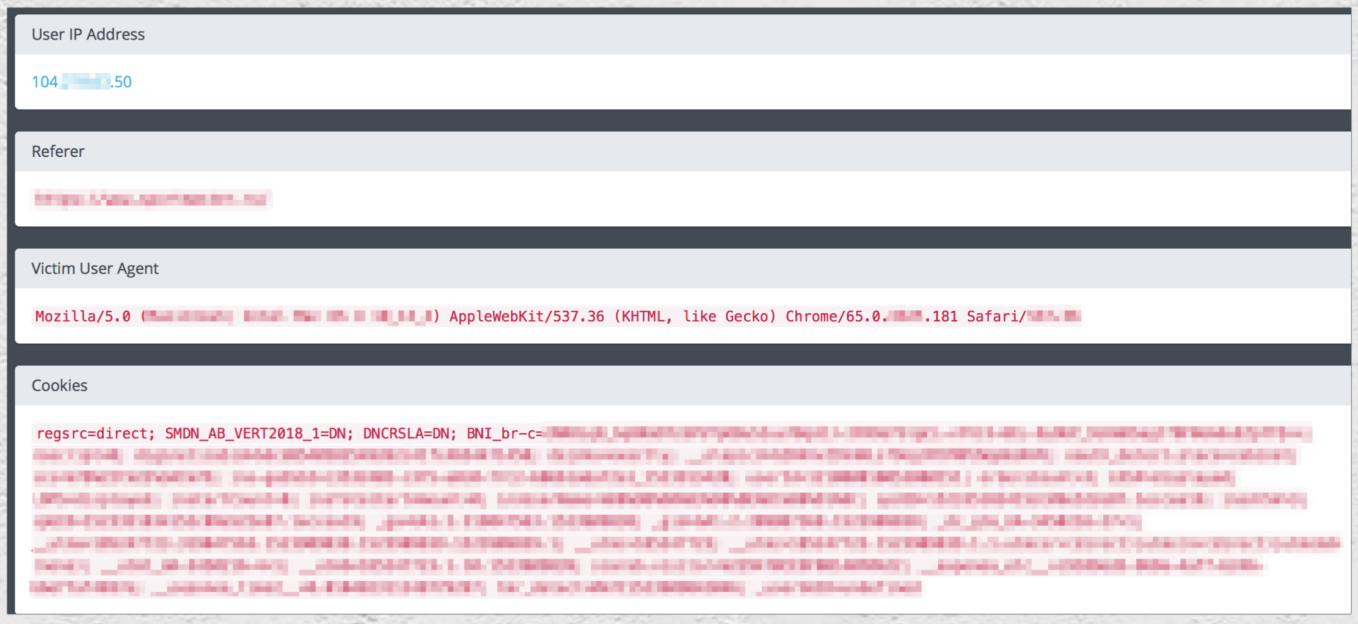


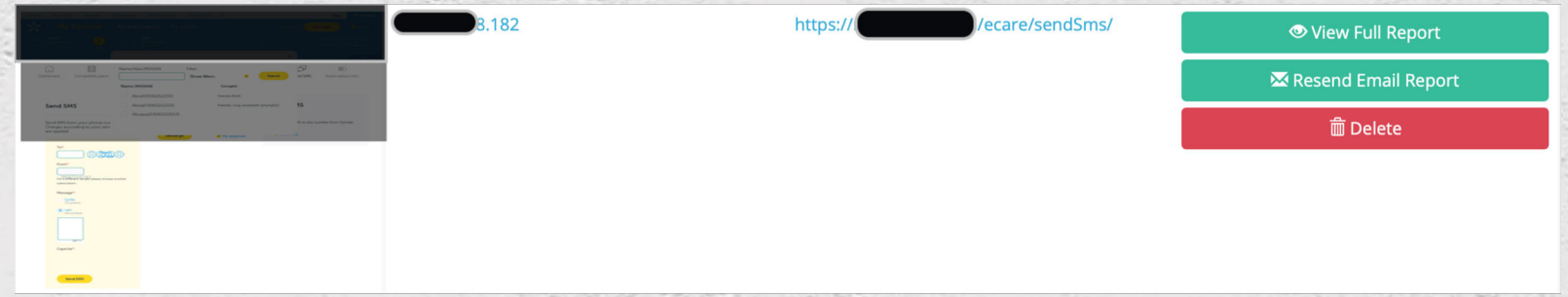
2³ EDITION

CALLBACK HANDLERS

HTTPS://XSSHUNTER.COM







2018.ZERONIGHTS.ORG

2^3 EDITION

CALLBACK HANDLERS

LAUNCH YOUR OWN COLLABORATOR SERVER:

HTTPS://BLOG.FABIOPIRES.PT/RUNNING-YOUR-INSTANCE-OF-BURP-COLLABORATOR-SERVER/

Running Your Instance of Burp Collaborator Server

APR 8, 2018

- A VPS(??). I bought one here.
- A domain name.
- LetsEncrypt.
- Burp Suite Pro.

ZERO NIGHTS 2018

2^3 EDITION

WHAT CAN BE SIMPLIFIED?

DAILY ROUTINE LOOKS LIKE:

1. INTERCEPT THE REQUEST
2. PUT PAYLOAD IN CORRECT HEADER/PARAMETER
3. SEND REQUEST
4. REPEAT N-TIMES B/C YOU NEVER KNOW WHAT WILL BE LOGGED AT BACKEND

ZERO NIGHTS 2018

2^3 EDITION

SHOULD WE PERFORM MANUAL CHECK ALL THE TIME?

ZERO NIGHTS 2018

2^3 EDITION

FEMIDA

BURP SUITE PLUGIN THAT:

- FLEXBLE AND EASY CONFIGURABLE
- PERFORMS ACCURATE PASSIVE CHECKS
- ACTIVE SCAN

WHO IS FEMIDA?

ZERO NIGHTS 2018

2^3 EDITION

FEMIDA

PLUGIN DEMO HERE

2^3 EDITION

TODO

- CSP REPORT DETECTOR AND REQUEST GENERATOR
- WAF DETECTOR
- ETC...

2³ EDITION

WE WISH YOU HAPPY HACKING

THANK YOU FOR ATTENTION

PLUGIN: HTTPS://GITHUB.COM/WISH-I-WAS/FEMIDA

FELL FREE TO ASK YOUR QUESTIONS:

TWITTER:

- HTTPS://TWITTER.COM/HD_421
- HTTPS://TWITTER.COM/WISH_IWAS

2018.ZERONIGHTS.ORG