

BLIND XSS & FEMIDA

PAVEL RUKAVISHNIKOV
HD



**ZERO
NIGHTS
2018**



ZERO
NIGHTS
2018

2³
EDITION

PAVEL RUKAVISHNIKOV

- CTF PLAYER
- PROGRAMMER

GITHUB: [HTTPS://GITHUB.COM/WISH-I-WAS](https://github.com/wish-i-was)

TWITTER: [HTTPS://TWITTER.COM/WISH_IWAS](https://twitter.com/wish_iwas)

HD

- SCRIPT KIDDIE
- BOUNTY HUNTER
- PENTESTER

GITHUB: [HTTPS://GITHUB.COM/HD421](https://github.com/HD421)

TWITTER: [HTTPS://TWITTER.COM/HD_421](https://twitter.com/HD_421)

WHOAMI



ZERO
NIGHTS
2018

2³
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

2³
EDITION

FEW FACTS ABOUT BLIND XSS?

- ALMOST ALWAYS IT'S STORED
- YOU CAN'T SEE ALERT(B37)
- NEED YOUR PATIENCE
- FACING IT THE OTHER WAY





ZERO
NIGHTS
2018

2³
EDITION

HEADERS:

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

WHERE TO INJECT

REQUEST PARAMETERS:

- IMAGINATION





ZERO
NIGHTS
2018

2³
EDITION

GROUND CONTROL

Secure Payment Info

MasterCard VISA AMEX DISCOVER PayPal

Name (as it appears on your card)
PAYLOAD

Card number (no dashes or spaces)

Expiration date
01 - January

Security code (3 on back, Amex: 4 on front)

Chat Invitation CLOSE X

Hello, my name is admin.
How can I help you today?

Chat Now

PAYLOAD

Full Name: **PAYLOAD**

Address Line 1: **PAYLOAD**
Street address, P.O. Box, company name, C/O

Address Line 2: **PAYLOAD**
Apartment, suite/unit, building, floor, etc.

City: **PAYLOAD**

State/Province/Region: **PAYLOAD**

ZIP/Postal Code: **PAYLOAD**

Country: **PAYLOAD**

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

2018.ZERONIGHTS.ORG



ZERO
NIGHTS
2018

2³
EDITION

Hello Super User,

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

- 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](#)



FEW MORE

Contact us

Name

Email

Phone Number

PAYLOAD

Send

PASSWORD

 PAYLOAD

Great

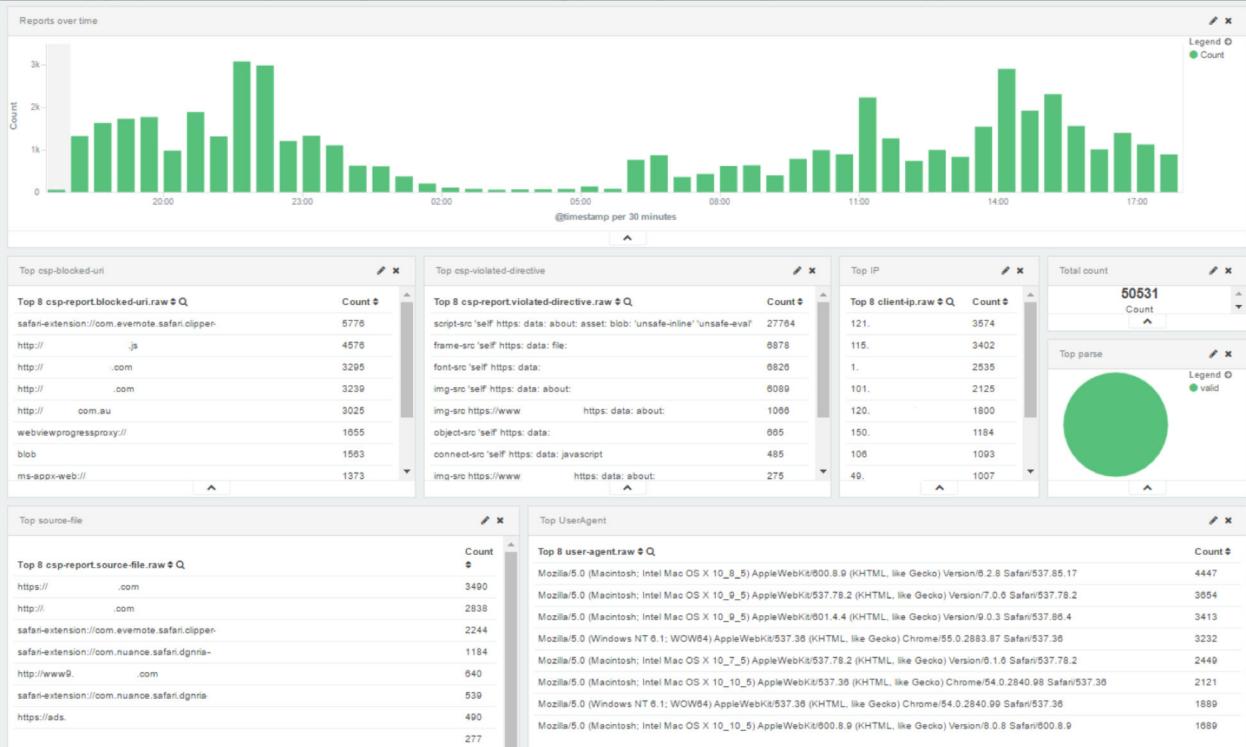
2018.ZERONIGHTS.ORG



ZERO
NIGHTS
2018

2³
EDITION

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



HOW IT LOOK SOMETIMES



ZERO
NIGHTS
2018

2³
EDITION

SHOULD I LOOK FOR IT?

^



24

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.mobub.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

2³
EDITION

CALLBACK HANDLERS

I DONT KNOW WHO YOU ARE OR WHAT
YOU WANT



BUT CALL ME MAYBE



ZERO
NIGHTS
2018

2³
EDITION

CALLBACK HANDLERS



2018.ZERONIGHTS.ORG



ZERO
NIGHTS
2018

2³
EDITION

CALLBACK HANDLERS

[HTTPS://GITHUB.COM/JOBERTABMA/GROUND-CONTROL](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

2³
EDITION

CALLBACK HANDLERS

[HTTPS://GITHUB.COM/SSL/EZXSS](https://github.com/SSL/ezXSS)

ezXSS v2.2
github.com/SSL/ezxss

Main

- Dashboard
- Settings
- Payload
- Reports**
- Reports
- Archived reports

Dashboard
Statistics of your ezXSS

1246 Total reports	54 Reports this week	5m Last report
74 Total domains	5 Domains this week	2 Total shared with you

Current status

Your version

Latests version

Update log of latests version

Download

Notepad

Here you can save some things for later, like a report id or a custom js.

Notepad

Save

2018.ZERONIGHTS.ORG



ZERO NIGHTS 2018

23
EDITION

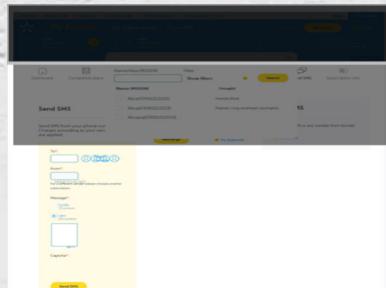
CALLBACK HANDLERS

[HTTPS://XSSHUNTER.COM](https://XSSHunter.com)

Custom `xss.htm` Subdomain

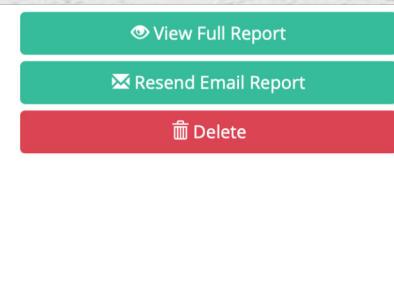
.xss.ht

User IP Address
104.16.16.50
Referer
https://www.google.com
Victim User Agent
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.332.181 Safari/537.36
Cookies
regsrc=direct; SMDN_AB_VERT2018_1=DN; DNCRSLA=DN; BNI_br-c=



3.182

[https://\[REDACTED\]/ecare/sendSms](https://[REDACTED]/ecare/sendSms)



2018.ZERONIGHTS.ORG



ZERO
NIGHTS
2018

2³
EDITION

CALLBACK HANDLERS

LAUNCH YOUR OWN COLLABORATOR SERVER:

[HTTPS://BLOG.FABIOPRIES.PT/RUNNING-YOUR-INSTANCE-OF-BURP-COLLABORATOR-SERVER/](https://blog.fabiopires.pt/running-your-instance-of-burp-collector-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

2³
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

2³
EDITION

SHOULD WE PERFORM MANUAL CHECK ALL THE TIME?



2018.ZERONIGHTS.ORG



ZERO
NIGHTS
2018

2³
EDITION

BURP SUITE PLUGIN THAT:

- FLEXIBLE AND EASY**
- CONFIGURABLE**
- PERFORMS ACCURATE**
- PASSIVE CHECKS**
- ACTIVE SCAN**

FEMIDA



WHO IS FEMIDA?

[2018.ZERONIGHTS.ORG](http://2018.zeronights.org)



ZERO
NIGHTS
2018

2³
EDITION

FEMIDA

PLUGIN DEMO HERE

2018.ZERONIGHTS.ORG



ZERO
NIGHTS
2018

2³
EDITION

TODO

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



ZERO
NIGHTS
2018

2³
EDITION

WE WISH YOU HAPPY
HACKING

THANK YOU FOR ATTENTION

PLUGIN: [HTTPS://GITHUB.COM/WISH-I-WAS/FEMIDA](https://github.com/wish-i-was/femida)

FELL FREE TO ASK YOUR QUESTIONS:

TWITTER:

- [HTTPS://TWITTER.COM/HD_421](https://twitter.com/HD_421)
- [HTTPS://TWITTER.COM/WISH_IWAS](https://twitter.com/wish_iwas)