Controlling the Source: Abusing Source Code Management Systems

Brett Hawkins (@h4wkst3r)
Adversary Simulation, IBM X-Force Red

X-Force Red

IBM

Agenda

- Introduction
- Source Code Management Systems
- GitHub Enterprise
- GitLab Enterprise
- Bitbucket
- SCMKit
- Demos
- Defensive Considerations
- Conclusion

Introduction

Who am I?

- **Current Role** – Adversary Simulation, IBM X-Force Red
- **Previous Roles** - Mandiant, J.P. Morgan Chase, J.M. Smucker Company
- **Conference Speaker** – DerbyCon, Wild West Hackin’ Fest, BSides, Hackers Teaching Hackers
- **Open-Source Tool Author** – SharPersist, DueDLLigence, InvisibilityCloak, SCMKit

How did this research come about?

- Real-world experience attacking source code management systems

- Recent Security Breaches
  - Software Supply Chain Attacks - SolarWinds, Kaseya, Codecov
  - Source Code Theft - LAPSUS$
    - Microsoft - Azure DevOps
    - T-Mobile - Bitbucket
    - Samsung - GitHub Enterprise
    - Globant - GitHub Enterprise

Research Goals

- Bring more attention to securing Source Code Management systems

- Inspire future research on defending Source Code Management systems

Attendee Takeaways

- Learn about different attack scenarios against Source Code Management systems
- Learn how to defend Source Code Management systems
- Learn how to abuse Source Code Management systems via privileged and non-privileged context

My Perspective

I AM:

- Current - Red Team Operator
- Previous - Blue Teamer

I AM NOT:

- DevOps Engineer
- Software Developer
- System Administrator

Source Code Management Systems

What is a Source Code Management System?

- Manages source code repositories
- Allows multiple developers to work on code at same time
- Supports integrations into other systems within DevOps pipeline

Popular Systems

- GitHub Enterprise

- GitLab Enterprise

- Bitbucket

DevOps Pipeline

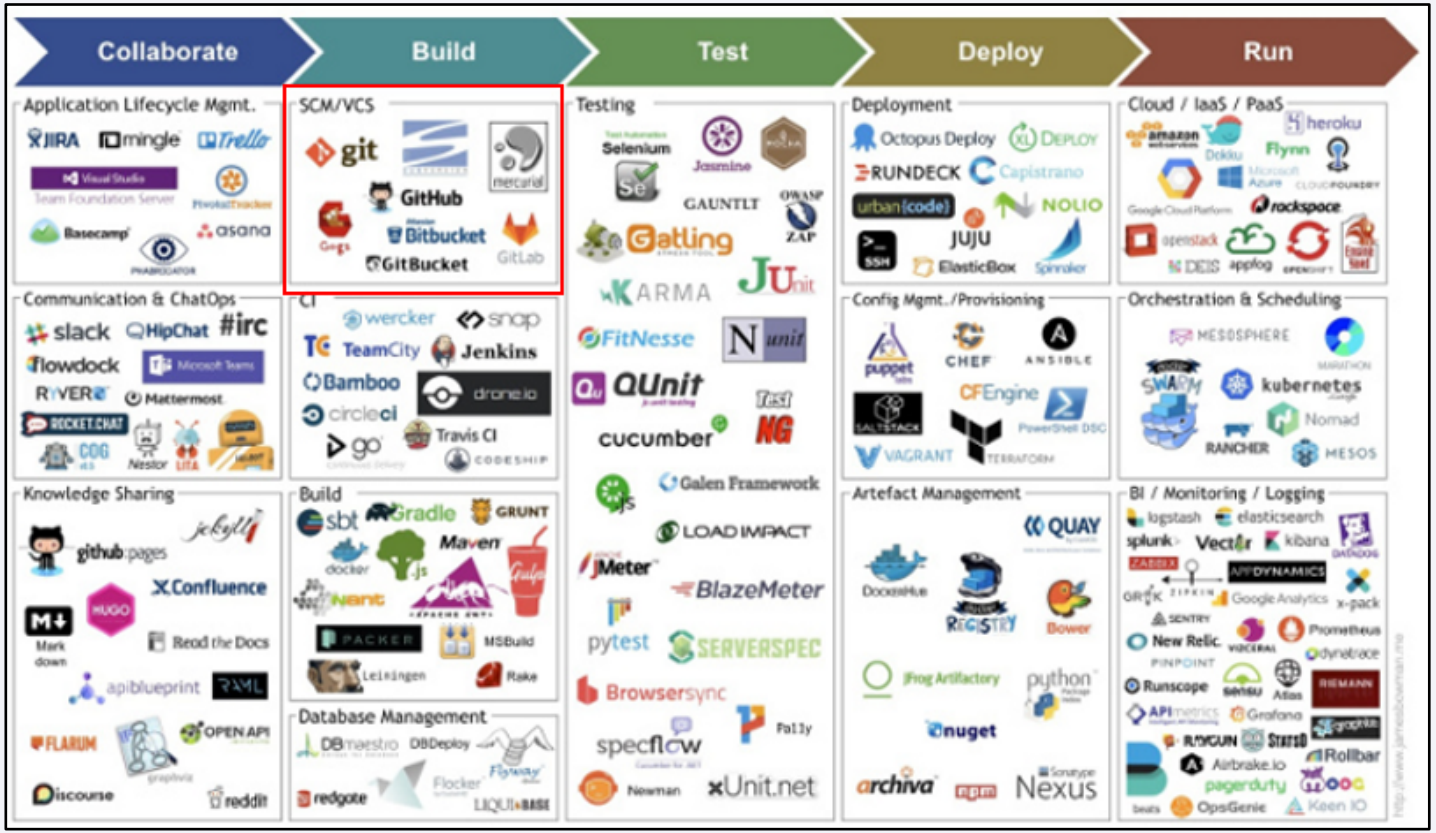


Image: https://medium.com/aws-cyber-range/secdevops-101-strengthen-the-basics-20f57197aa1c

Software Supply Chain Attacks

- Attacker injects itself into development process to deploy malicious code
- Research focuses on scenarios “B” and “C” below

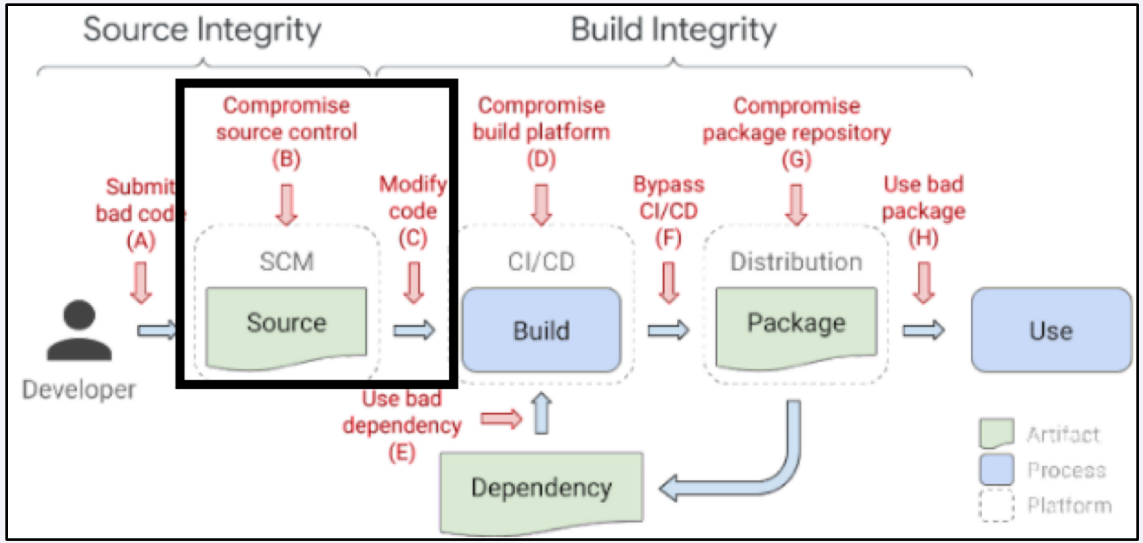


Image: https://opensource.googleblog.com/2021/10/protect-your-open-source-project-from-supply-chain-attacks.html

Lateral Movement to other DevOps Systems

SCM Systems

- Initial access point
- Pivot to:
  - CI/CD Platform
  - Distribution Platform

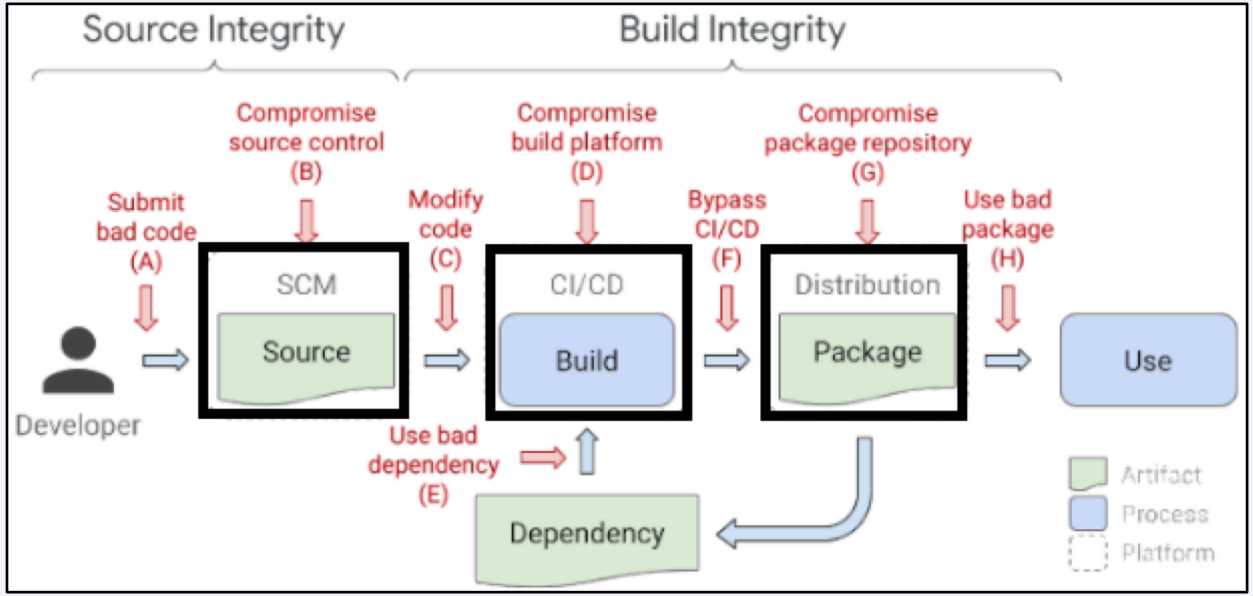


Image: https://opensource.googleblog.com/2021/10/protect-your-open-source-project-from-supply-chain-attacks.html

GitHub Enterprise

Access Model

Enterprise Roles

- Owners, Members

Organization Roles

- Organization Owners, Organization Members, Security Managers, GitHub App Managers, Outside Collaborators

Repository Roles

- Read, Triage, Write, Maintain, Admin

Access Token Scopes

- Repository, Organization, SSH Keys, Gists, Users, GPG Keys, Site Admin

API Capabilities

- REST API

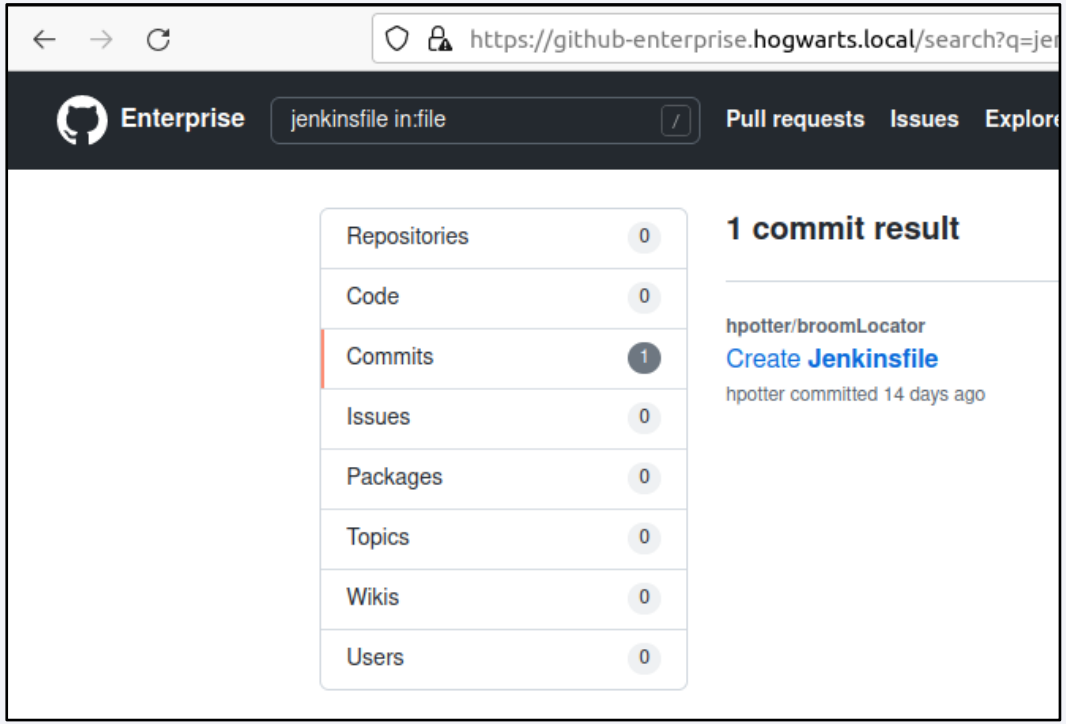
- Interact with:
  - Repositories
  - SSH Keys
  - Users
  - Admin functionality
  - And much more…

Attack Scenarios

Attack Scenario	Sub-Scenario	Admin Required?
Reconnaissance	-Repository -File -Code	No
Repository Takeover	N/A	Yes
User Impersonation	-Impersonate User Login -Impersonation Token	Yes
Promoting User to Site Admin	N/A	Yes
Maintain Persistent Access	-Personal Access Token -Impersonation Token -SSH Key	No Yes No
Management Console Access	N/A	Yes

Reconnaissance

- Web interface or REST API
  - Repository, File, Code



Reconnaissance Logging

HAProxy Log

- /var/log/haproxy.log

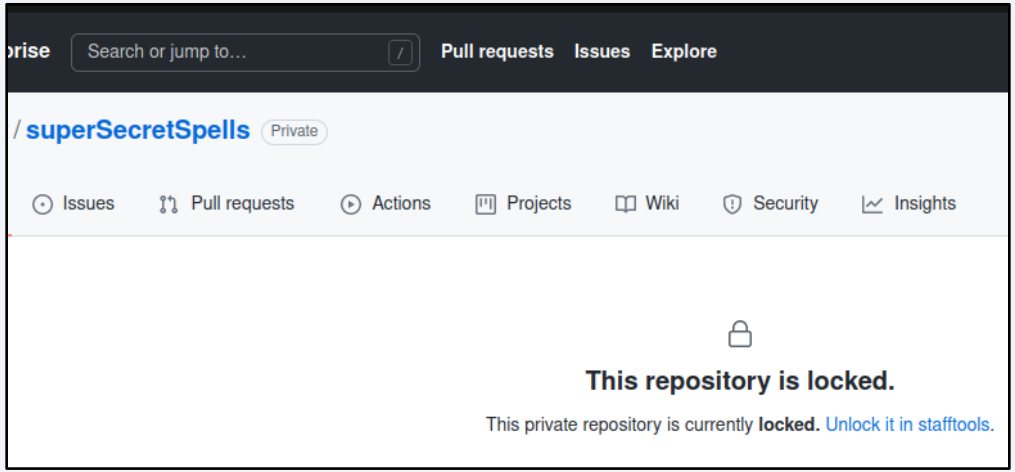
Search Criteria

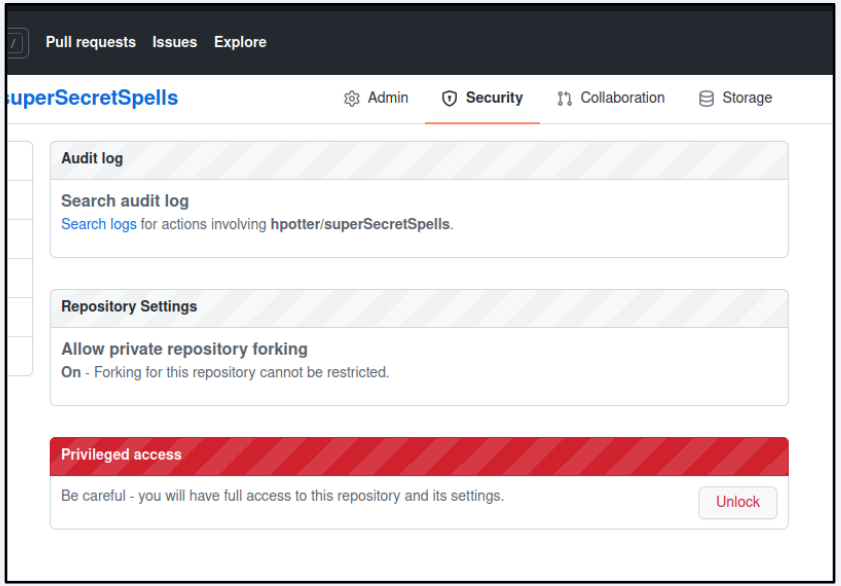
- ('/search' OR '/api/v3/search') AND 'http'

```
https://github-enterprise.hogwarts.local/api/v3/search/code /api/v3/search/code?q=jenkinsfile%20in:file"
https://github-enterprise.hogwarts.local/api/v3/search/code /api/v3/search/code?q=jenkinsfile&in:file"
https://github-enterprise.hogwarts.local/api/v3/search/code /api/v3/search/code?q=jenkinsfile"
https://github-enterprise.hogwarts.local/api/v3/search/code /api/v3/search/code?q=Jenkinsfile"
https://github-enterprise.hogwarts.local/api/v3/search/commits /api/v3/search/commits?q=jenkinsfile"
https://github-enterprise.hogwarts.local/api/v3/search/code /api/v3/search/code?q=password"
https://github-enterprise.hogwarts.local/api/v3/search/code /api/v3/search/code?q=ssword"
https://github-enterprise.hogwarts.local/api/v3/search/code /api/v3/search/code?q=pas"
https://github-enterprise.hogwarts.local/api/v3/search/code /api/v3/search/code?q=pass"
https://github-enterprise.hogwarts.local/api/v3/search/code /api/v3/search/code?q=passw"
https://github-enterprise.hogwarts.local/api/v3/search/code /api/v3/search/code?q=passwo"
https://github-enterprise.hogwarts.local/api/v3/search/code /api/v3/search/code?q=passwor"
https://github-enterprise.hogwarts.local/api/v3/search/code /api/v3/search/code?q=password"
https://github-enterprise.hogwarts.local/api/v3/search/code /api/v3/search/code?q=word"
```

Repository Takeover

- Site admin can unlock any repository for modify access





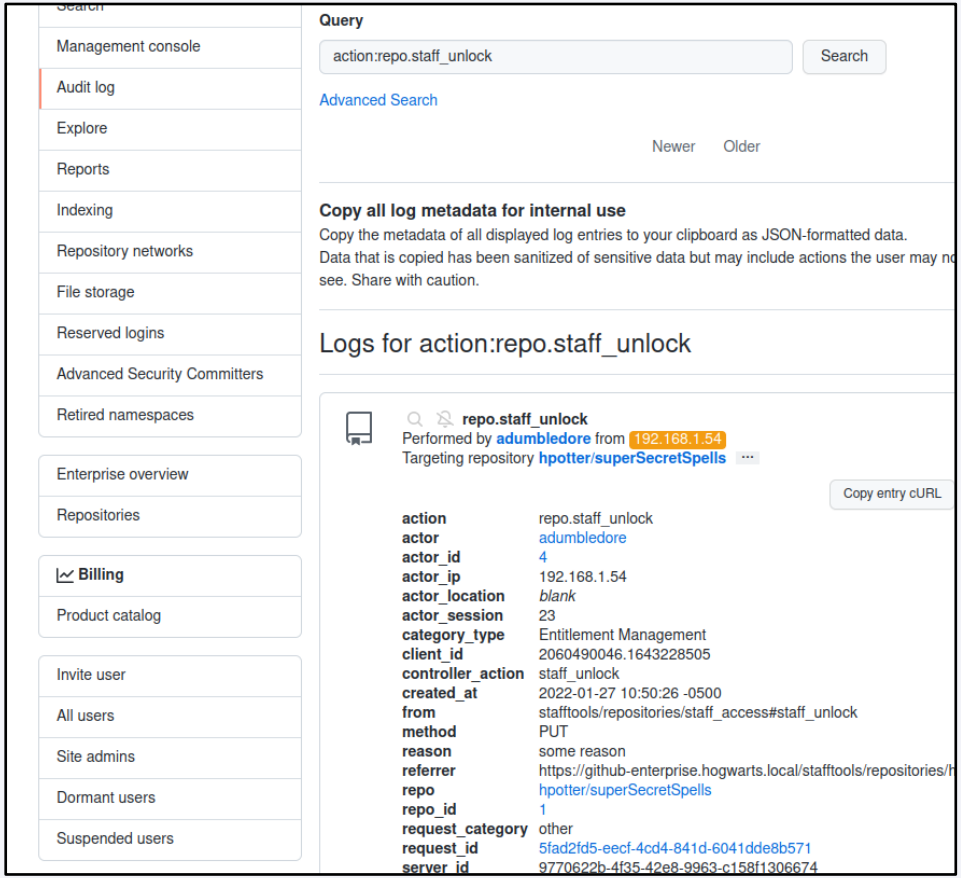
Repository Takeover Logging

Audit Log

- /var/log/github-audit.log

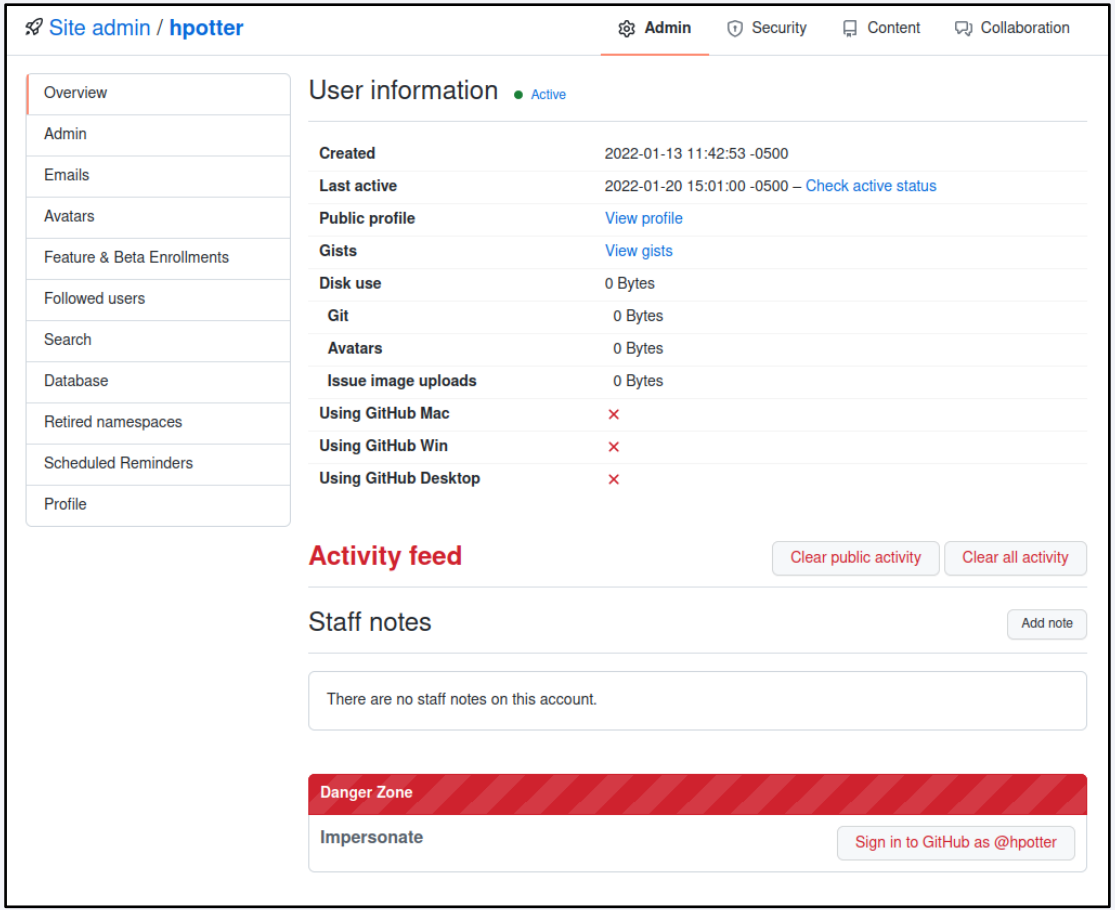
Search Criteria

- action:repo.staff_unlock



User Impersonation

- Impersonate User Login
- Impersonation Token



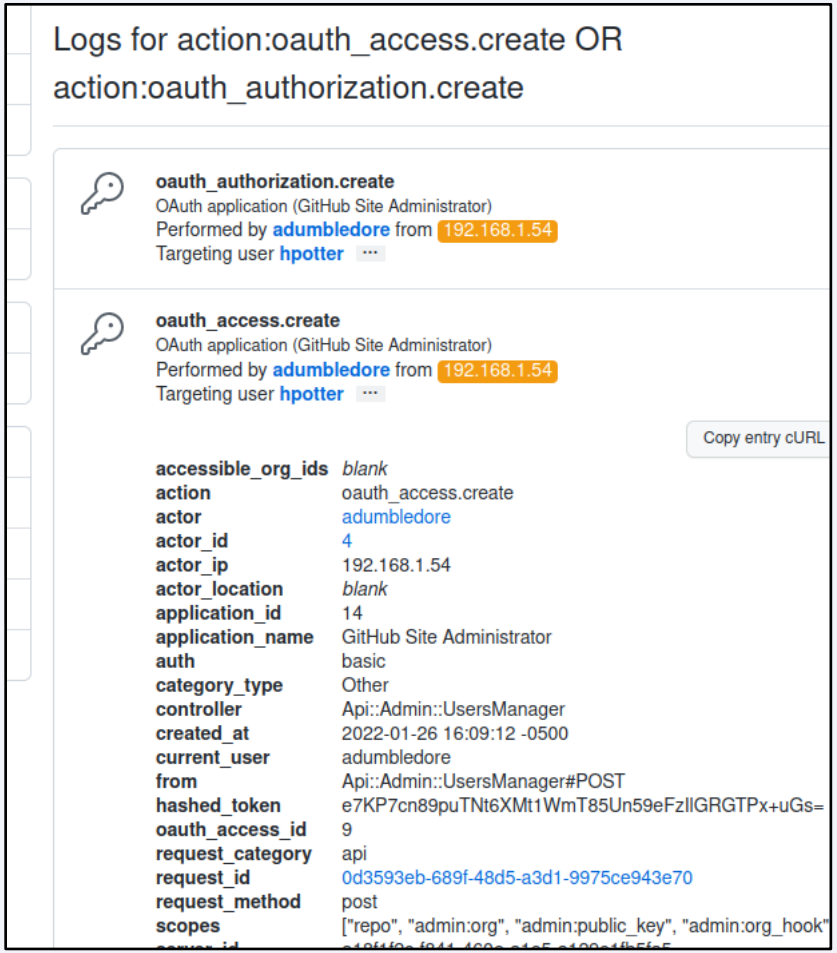
User Impersonation Logging

Audit Log

- /var/log/github-audit.log

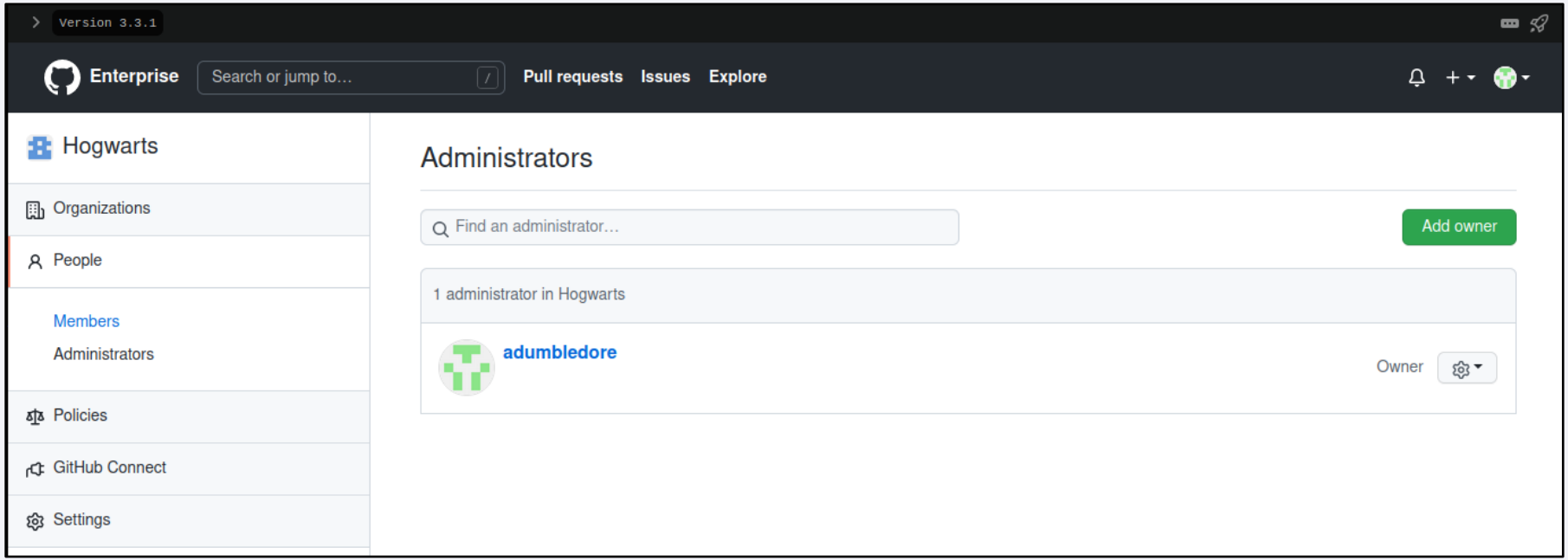
Search Criteria

- action:staff.fake_login
- action:oauth_access.create
- action:oauth_authorization.create



Promoting User to Site Admin

- Using site admin privileges, add any user to site admin



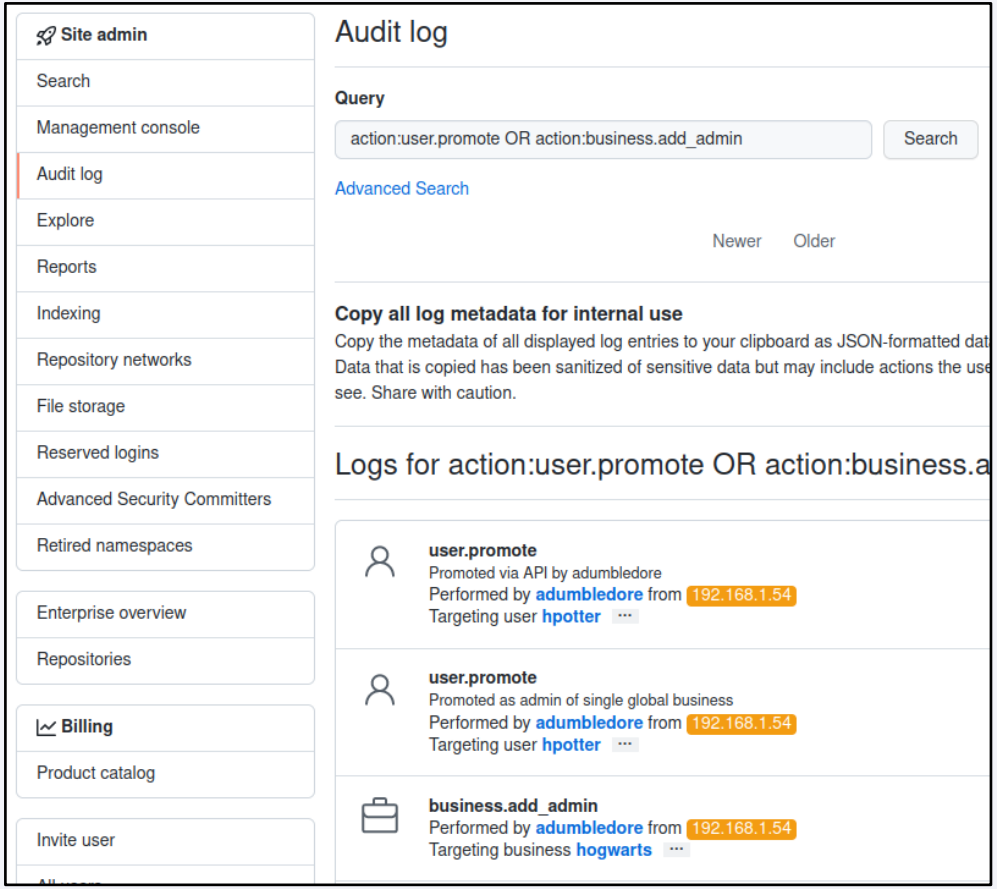
Promoting User to Site Admin Logging

Audit Log

- /var/log/github-audit.log

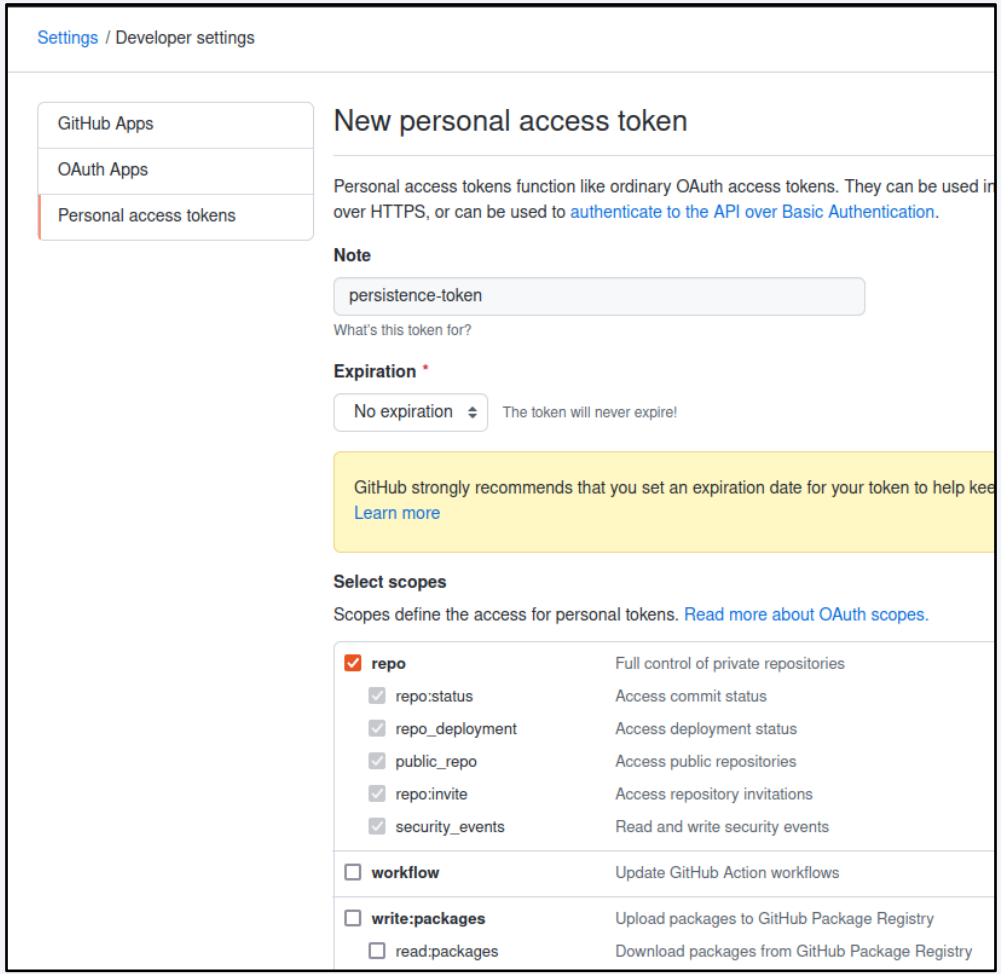
Search Criteria

- action:user.promote
- action:business.add_admin



Maintain Persistent Access

- Personal Access Token
- Impersonation Token
- SSH Key



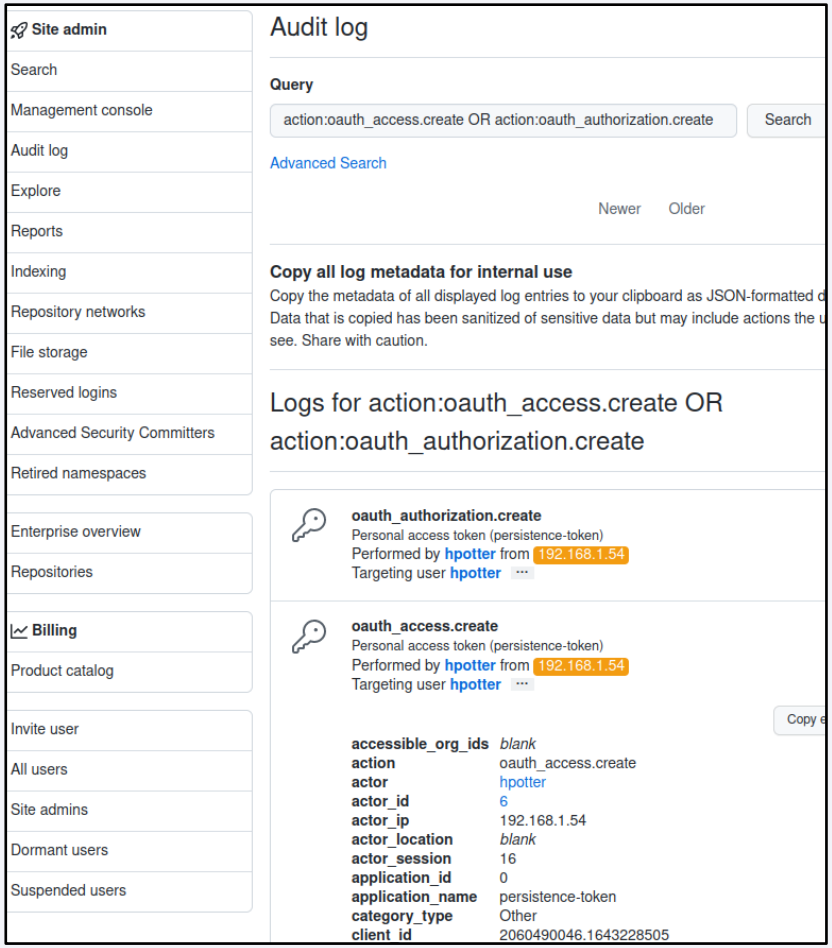
Maintain Persistent Access Logging

Audit Log

- /var/log/github-audit.log

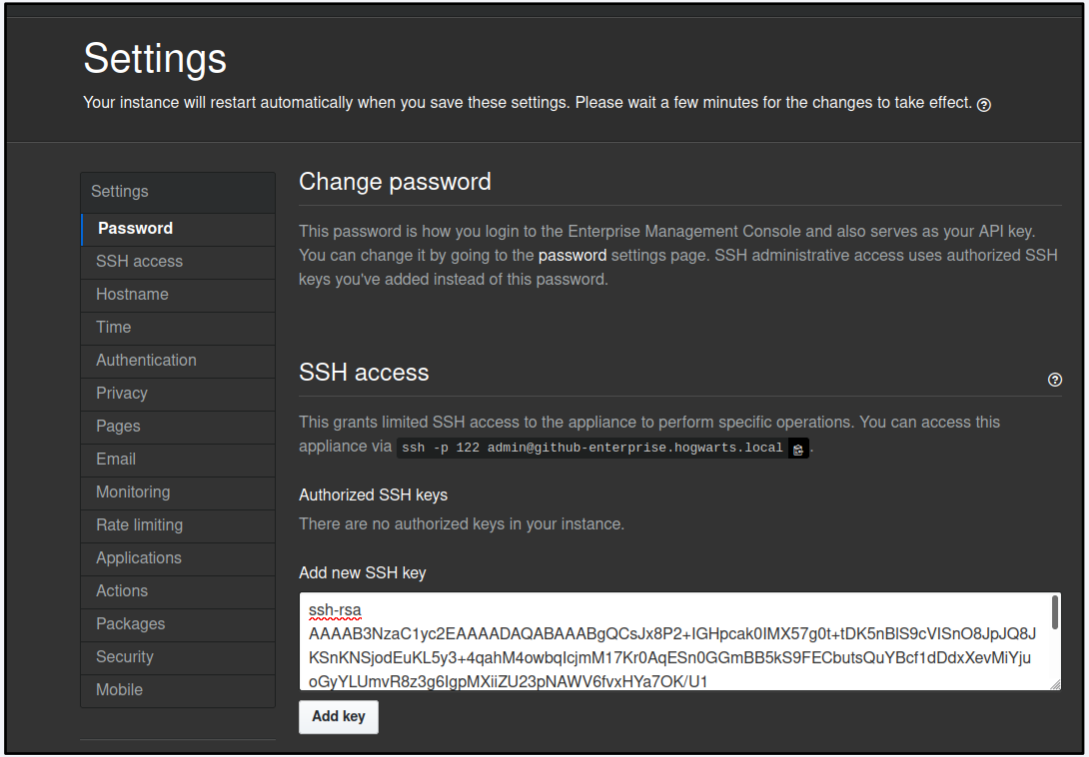
Search Criteria

- action:oauth_access.create
- action:oauth_authorization.create
- action:public_key.create
- action:public_key.verify



Management Console Access

- Single shared password
- Configure enterprise instance
  - Example: Adding SSH key



Management Console Access

- Multiple commands available in management console SSH access
  - Example: `ghe-config -l`

```
[10:08:08] hawk@ubuntu-demo:~$ ssh -i test_ssh_key admin@github-enterprise.hogwarts.local -p 122

Administrative shell access is permitted for troubleshooting and performing
documented operations procedures only. Modifying system and application files,
running programs, or installing unsupported software packages may void your
support contract. Please contact GitHub support at https://support.github.com
if you have a question about the activities allowed by your support contract.

INFO: Release version: 3.3.1
INFO: 2 CPUs, 15GB RAM on VMWare
INFO: License: evaluation; Seats: unlimited; Will expire in 31 days.
WARN: Load average: 3.15 3.57 4.86 (3.15 > 2 CPUs)
INFO: Usage for root disk: 22G of 98G (24%)
INFO: Usage for user data disk: 14G of 20G (71%)
INFO: TLS: enabled; Certificate will expire in 351 days.
INFO: HA: standalone
INFO: Configuration run in progress: false
Last login: Wed Jan 19 14:56:25 2022 from 192.168.1.51
admin@github-enterprise-hogwarts-local:~$
```

Management Console Access Logging

Management Log

- /var/log/enterprise-manage/unicorn.log

```
 | grep -i authorized-keys | grep -i post
/2022:15:08:01 +0000] "POST /setup/settings/authorized-keys HTTP/1.0" 201 653 0.300
```

GitLab Enterprise

Access Model

User Project Permissions

- Guest, Reporter, Developer, Maintainer, Owner

Access Token Scopes

- api, read_user, read_api, read_repository, write_repository, read_registry, write_registry, sudo

API Capabilities

- REST API

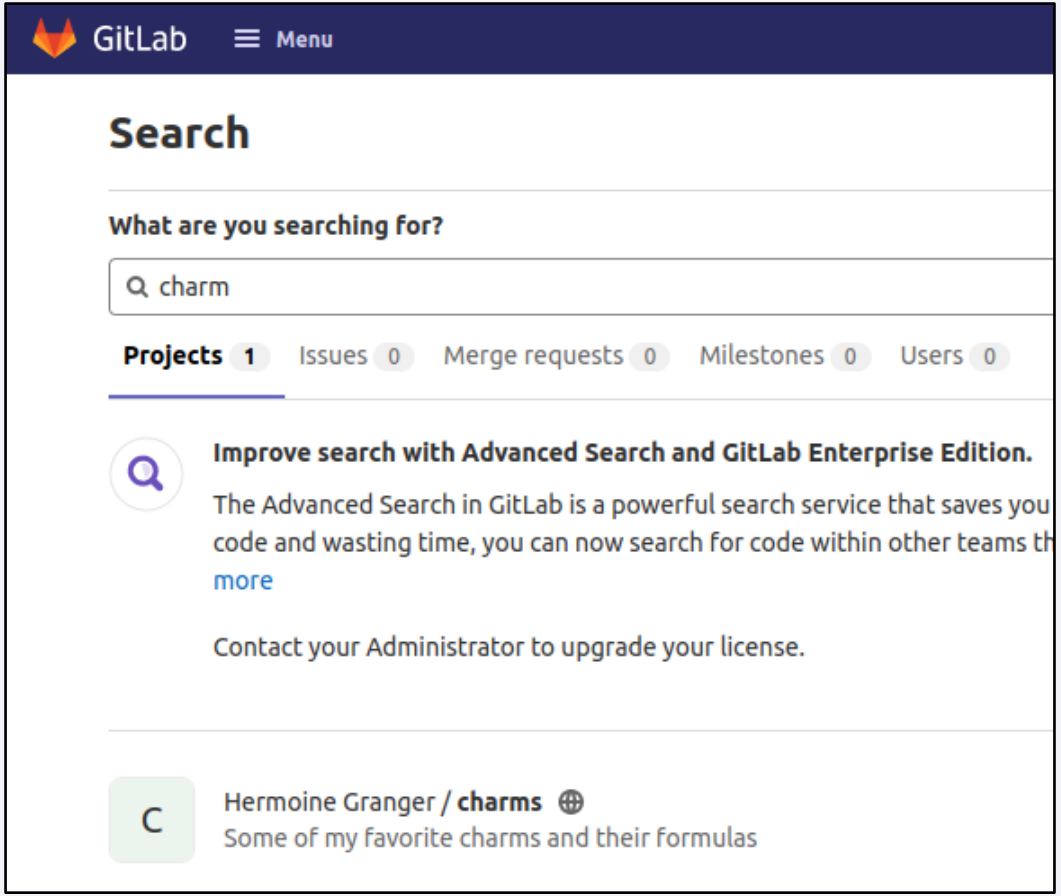
- Interact with:
  - Repositories
  - SSH Keys
  - Users
  - Admin functionality
  - And much more…

Attack Scenarios

Attack Scenario	Sub-Scenario	Admin Required?
Reconnaissance	-Repository -File -Code	No
User Impersonation	-Impersonate User Login -Impersonation Token	Yes
Promoting User to Admin Role	N/A	Yes
Maintain Persistent Access	-Personal Access Token -Impersonation Token -SSH Key	No Yes No
Modifying CI/CD Pipeline	N/A	Yes – Project Level
SSH Access	N/A	Yes

Reconnaissance

- Web interface or REST API
  - Repository, File, Code



Reconnaissance Logging

Production Log

- /var/log/gitlab/gitlab-rails/production.log
- /var/log/gitlab/gitlab-rails/production_json.log

API Log

- /var/log/gitlab/gitlab-rails/api_json.log

Access Log

- /var/log/gitlab/nginx/gitlab_access.log

Search Criteria

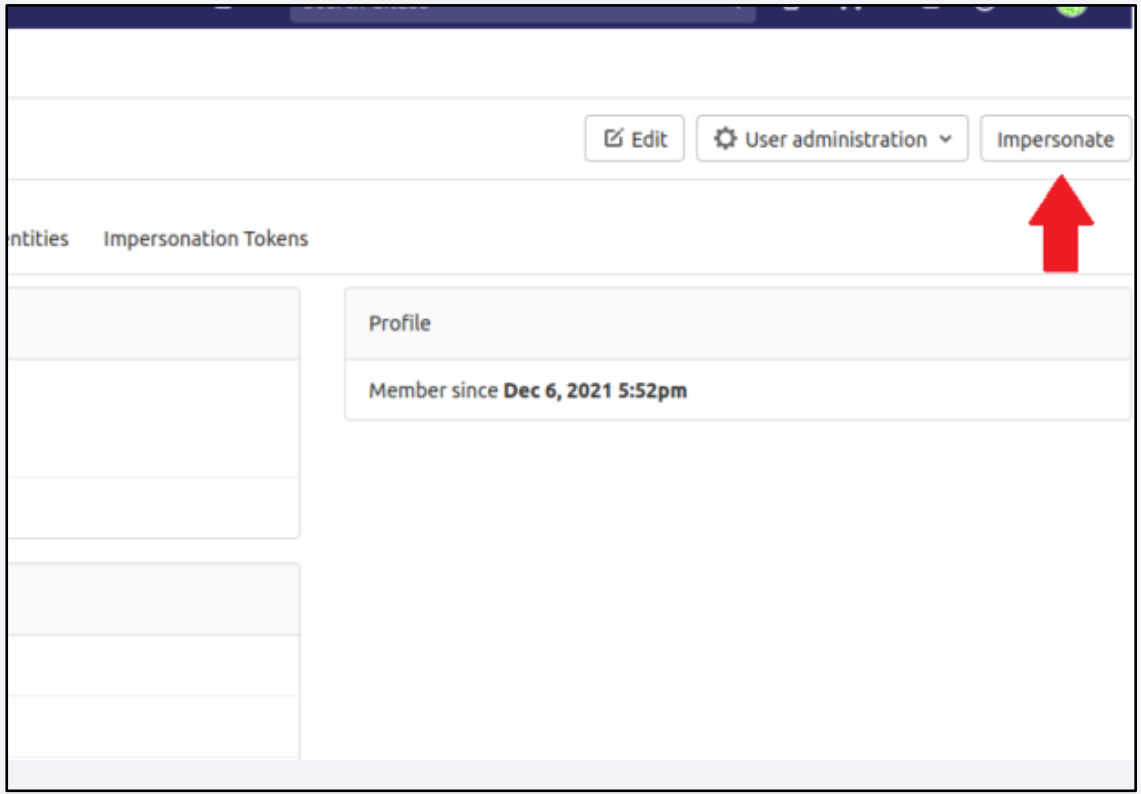
- 'get' AND '/search?search'
- 'get' AND '/search'
- 'get' AND ('/search'| OR 'repository/tree')
- 'search'

```
root@gitlab-server:~# cat /var/log/gitlab/gitlab-ra
Started GET "/search?search=[FILTERED]&group_id=&pr
root@gitlab-server:~#
root@gitlab-server:~#
root@gitlab-server:~# cat /var/log/gitlab/gitlab-ra
{"method":"GET","path":"/search","format":"html","c
alue":"false"},{"key":"repository_ref","value":""},
ta.client_id":"user/2","meta.search.group_id":"","m
otter","ua":"Mozilla/5.0 (X11; Ubuntu; Linux x86_64
e_calls":18,"redis_cache_duration_s":0.007068,"redi
count":0,"db_cached_count":24,"db_replica_count":0,
b_primary_duration_s":0.023,"cpu_s":0.308263,"mem_o
root@gitlab-server:~# _
```

```
root@gitlab-server:~# cat /var/log/gitlab/nginx/gitlab_access.log | grep -i '/search' |
192.168.1.54 [27/Jan/2022:15:49:28 /api/v4/search?scope=projects
192.168.1.54 [27/Jan/2022:15:50:12 /api/v4/search?scope=projects&search=charm
192.168.1.54 [27/Jan/2022:15:50:22 /api/v4/search?scope=projects&search=charm
192.168.1.54 [27/Jan/2022:16:09:07 /api/v4/search?scope=blobs&search=jenkinsfile
192.168.1.54 [27/Jan/2022:16:21:08 /api/v4/projects/7/search?scope=blobs&keyword=whoami
192.168.1.54 [27/Jan/2022:16:21:44 /api/v4/projects/7/search?scope=blobs&search=whoami
192.168.1.54 [27/Jan/2022:16:24:13 /api/v4/projects/7/search?scope=commits&search=jenkin
```

User Impersonation

- Impersonate User Login
- Impersonation Token



User Impersonation Logging

Production Log

- /var/log/gitlab/gitlab-rails/production_json.log
- /var/log/gitlab/gitlab-rails/production.log

API Log

- /var/gitlab/gitlab-rails/api_json.log

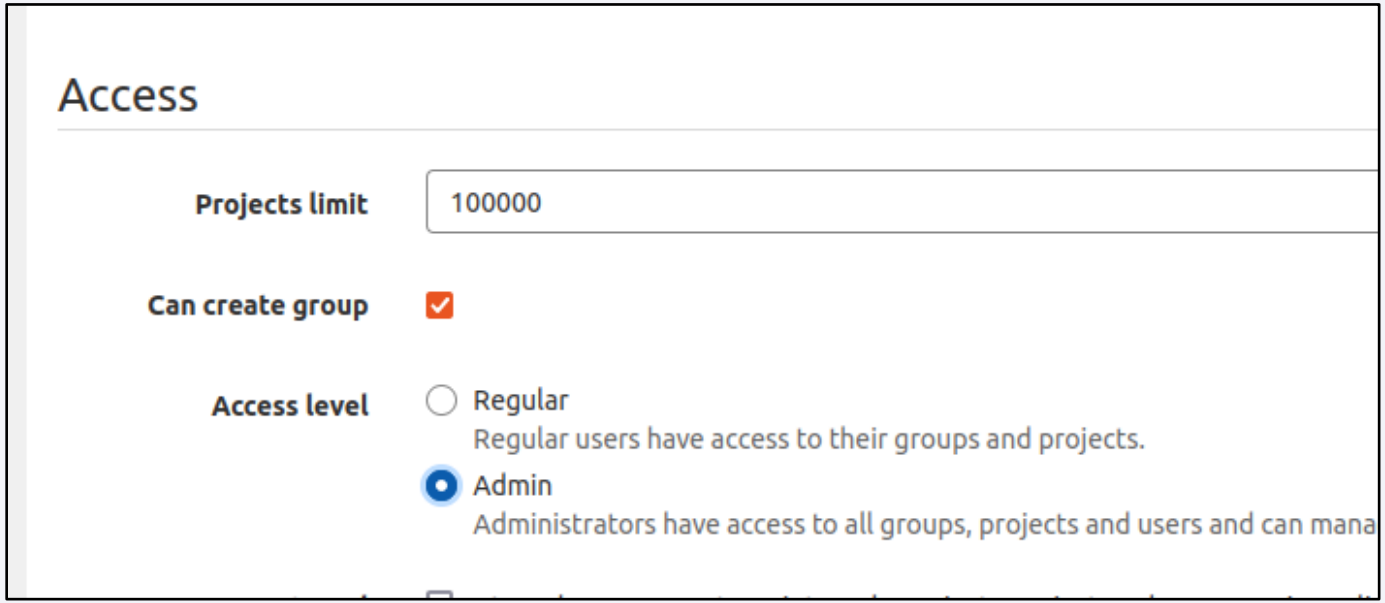
Search Criteria

- 'has started impersonating'
- 'impersonate'
- 'post' AND 'impersonation_tokens'
- 'impersonation_tokens'

```
og/gitlab/gitlab-rails/api_json.log | grep -i impersonation_tokens
Z","severity":"INFO","duration_s":0.04186,"db_duration_s":0.01345,"view_
lue":["api,read_user,read_api,read_repository,write_repository,sudo"]}],
message\":{\"scopes\":[\"can only contain available scopes\"]}}"],"queue
is_cache_write_bytes":100,"redis_shared_state_calls":2,"redis_shared_sta
_cached_count":0,"db_primary_count":9,"db_primary_cached_count":4,"db_pr
":5063695,"pid":9154,"correlation_id":"01FTEBPMAN9D35EHMJ7HX50WRS","meta
:"user/5","content_length":"107","request_urgency":"default","target_dur
Z","severity":"INFO","duration_s":0.03545,"db_duration_s":0.0059,"view_c
ue":["api"]}],"host":"gitlab.hogwarts.local","remote_ip":"192.168.1.54,
dis_read_bytes":125,"redis_write_bytes":557,"redis_cache_calls":5,"redis
t":15,"db_write_count":3,"db_cached_count":4,"db_replica_count":0,"db_re
tion_s":0.0,"db_primary_duration_s":0.009,"cpu_s":0.054021,"mem_objects"
r_id/impersonation_tokens","meta.remote_ip":"192.168.1.54","meta.feature
Z","severity":"INFO","duration_s":0.02669,"db_duration_s":0.00377,"view_
lue":["api","read_user","read_repository","write_repository","sudo"]}],"
:0.00594,"redis_calls":4,"redis_duration_s":0.002306,"redis_read_bytes":
01755,"redis_shared_state_write_bytes":101,"db_count":13,"db_write_count
:0,"db_primary_wal_cached_count":0,"db_replica_duration_s":0.0,"db_prima
e","meta.caller_id":"POST /api/:version/users/:user_id/impersonation_tok
```

Promoting User to Admin Role

- Using admin privileges, add any user to admin



Promoting User to Admin Role Logging

Production Log

- /var/log/gitlab/gitlab-rails/production_json.log
- /var/log/gitlab/gitlab-rails/production.log

API Log

- /var/log/gitlab/gitlab-rails/api_json.log

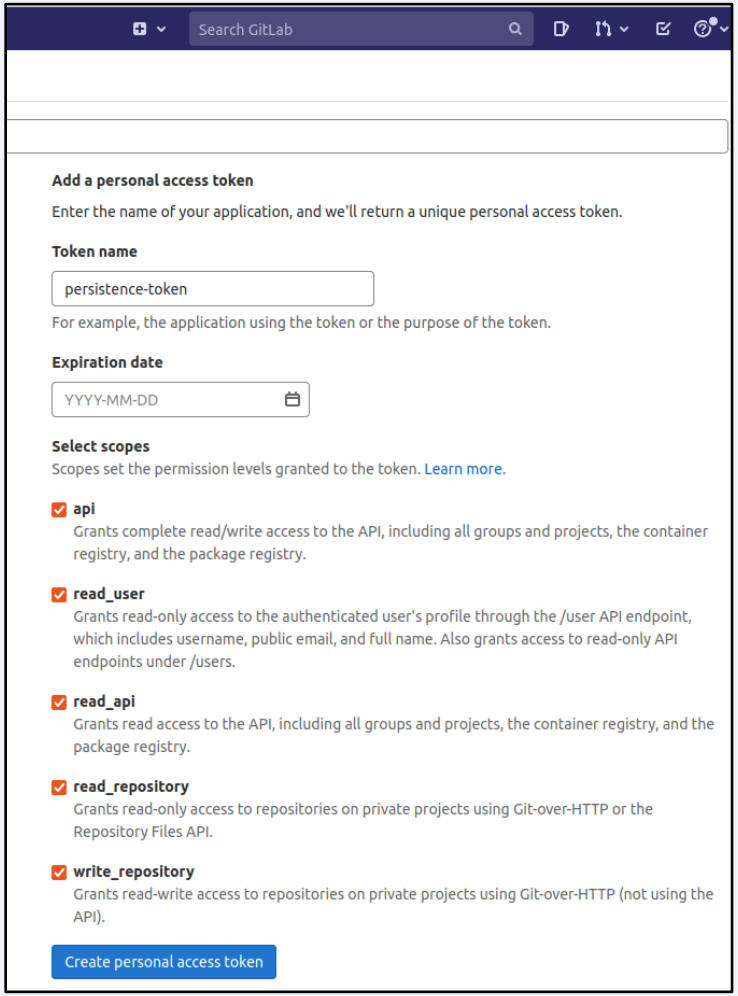
Search Criteria

- 'patch' AND 'admin/users'
- 'put' AND '"key":"admin","value":"true"'

```
/gitlab-rails/api_json.log | grep -i PUT | grep -i '"key":"admin","value":"true"
ity":"INFO","duration_s":0.07148,"db_duration_s":0.01323,"view_duration_s":0.058
"/api/:version/users/:id","user_id":5,"username":"adumbledore","queue_duration_s
":442,"redis_cache_write_bytes":225,"redis_shared_state_calls":2,"redis_shared_s
replica_wal_cached_count":0,"db_primary_count":25,"db_primary_cached_count":7,"d
total_bytes":3051975,"pid":12594,"correlation_id":"01FTEDXJNK2MRNS3QN64KJBQ8W","
rgency":"default","target_duration_s":1}
```

Maintain Persistent Access

- Personal Access Token
- Impersonation Token
- SSH Key



Maintain Persistent Access Logging

Production Log

- /var/log/gitlab/gitlab-rails/production_json.log
- /var/log/gitlab/gitlab-rails/production.log

API Log

- /var/log/gitlab/gitlab-rails/api_json.log

Search Criteria

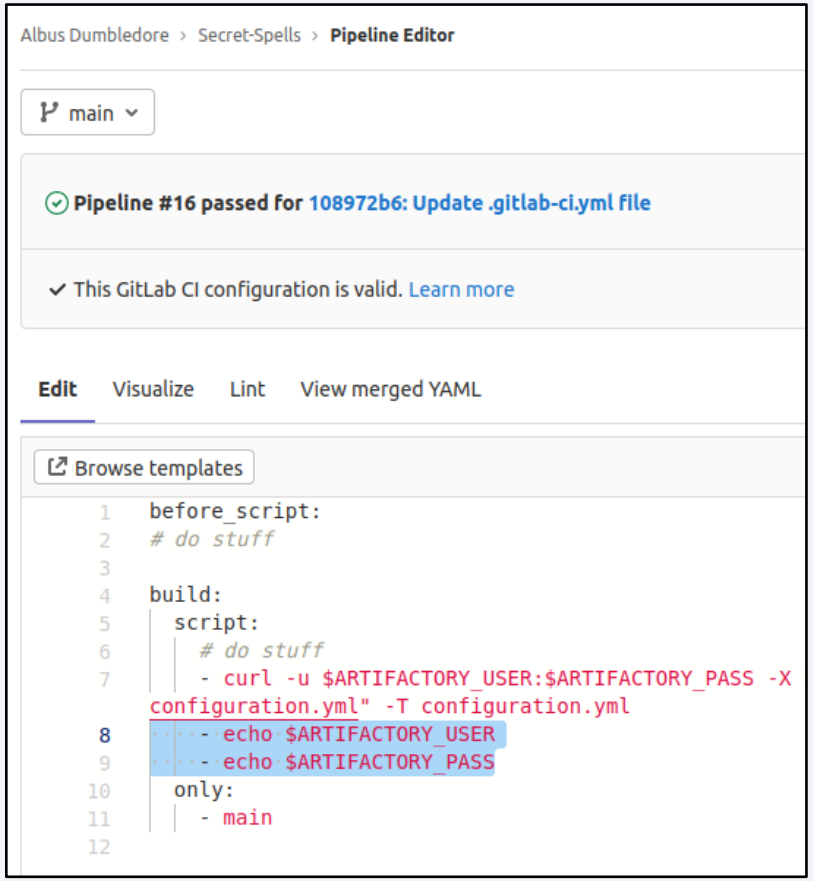
- 'post' AND 'personal_access_tokens'
- 'post' AND 'profile/keys'
- 'post' AND 'personal_access_tokens'
- 'post' AND 'user/keys'

```
r:~# cat /var/log/gitlab/gitlab-rails/production.log | grep -A3 -i pos
profile/personal_access_tokens" for 192.168.1.54 at 2022-01-27 14:03:2
files::PersonalAccessTokensController#create as HTML
uthenticity_token"=>"[FILTERED]", "personal_access_token"=>"[FILTERED]
ps://gitlab.hogwarts.local/-/profile/personal_access_tokens
r:~#
r:~#
r:~# cat /var/log/gitlab/gitlab-rails/production_json.log | grep -i po
"path":"/-/profile/personal_access_tokens","format":"html","controller
authenticity_token","value":"[FILTERED]"},{"key":"personal_access_toke
```

```
'api_json.log | grep -i post | grep -i 'user/keys'
luration_s":0.01929,"db_duration_s":0.00046,"view_duration_s":0.01883,"st
.S9cVISnO8JpJQ8JKSnKNSjodEuKL5y3 4qahM4owbqIcjmM17Kr0AqESn0GGmBB5kS9FECbu
)C93 LEqMu0IidE/AgiJP/p3QQr4WRnGvErNbgJIPU1IHeHA7wSxgC/o4btbrkfoy0ykLf3nT
.68.1.54, 127.0.0.1","ua":"curl/7.68.0","route":"/api/:version/user/keys'
int":1,"db_primary_cached_count":0,"db_primary_wal_count":0,"db_primary_w
.d":"01FTEHE2Z6GTKM2570GBC086V1","meta.caller_id":"POST /api/:version/use
```

Modifying CI/CD Pipeline

- Modify `.gitlab-ci.yml` file in repo
- Triggers pipeline to run for that project



Modifying CI/CD Pipeline Logging

Production Log

- /var/log/gitlab/gitlab-rails/production_json.log

Search Criteria

- 'post' AND '/api/graphql' AND '.gitlab-ci.yml' AND 'update'

```
root@gitlab-server:~# cat /var/log/gitlab/gitlab-rails/production_json.log | grep -i post | grep -i '/api/graphql' | grep -i '.gitl
{"method":"POST","path":"/api/graphql","format":"*/*","controller":"GraphqlController","action":"execute","status":200,"time":"2022
"mutation commitCIFile($action: CommitActionMode!, $projectPath: ID!, $branch: String!, $startBranch: String, $message: String!, $f
anch: $startBranch, message: $message, actions: [{action: $action, filePath: $filePath, lastCommitId: $lastCommitId, content: $cont
","value":{"operationName":"commitCIFile","variables":"[FILTERED]","query":"mutation commitCIFile($action: CommitActionMode!, $proj
mitCreate(\n    input: {projectPath: $projectPath, branch: $branch, startBranch: $startBranch, message: $message, actions: [{action
 commitPipelinePath\n    errors\n    __typename\n  }\n}\n"}}],"correlation_id":"01FTER04J41TTE6CF315A4CX9T","meta.user":"adumbledor
user/5","graphql":[{"depth":3,"complexity":7,"used_fields":["Commit.sha","Commit.__typename","CommitCreatePayload.commit","CommitCr
:[],"variables":"{\"action\"=>\"UPDATE\", \"projectPath\"=>\"adumbledore/secret-spells\", \"branch\"=>\"main\", \"startBranch\"=>\"
b69a5c68931691df57c69e884a0cfca8f\"}","operation_name":"commitCIFile"}],"remote_ip":"192.168.1.54","user_id":5,"username":"adumbled
```

SSH Access

GitLab Config file

- /etc/gitlab/gitlab.rb

GitLab Secrets file

- /etc/gitlab/gitlab-secrets.json

```
gitlab@gitlab-server:~$ sudo cat /etc/gitlab/gitlab.rb | grep -i bind_dn -B5 -A5
[sudo] password for gitlab:
#   main: # 'main' is the GitLab 'provider ID' of this LDAP server
#     label: 'LDAP'
#     host: '_your_ldap_server'
#     port: 389
#     uid: 'sAMAccountName'
#     bind_dn: '_the_full_dn_of_the_user_you_will_bind_with'
#     password: '_the_password_of_the_bind_user'
#     encryption: 'plain' # "start_tls" or "simple_tls" or "plain"
#     verify_certificates: true
#     smartcard_auth: false
#     active_directory: true
--
#   secondary: # 'secondary' is the GitLab 'provider ID' of second LDAP server
#     label: 'LDAP'
#     host: '_your_ldap_server'
#     port: 389
#     uid: 'sAMAccountName'
#     bind_dn: '_the_full_dn_of_the_user_you_will_bind_with'
#     password: '_the_password_of_the_bind_user'
#     encryption: 'plain' # "start_tls" or "simple_tls" or "plain"
#     verify_certificates: true
#     smartcard_auth: false
#     active_directory: true
```

Postgresql DB -

```
gitlabhq_production=> select id,username,encrypted_password,admin,state,otp_required_for_login,otp_backup_
 id |   username   |                    encrypted_password                    | admin | state  | otp_re
----+--------------+----------------------------------------------------------+-------+--------+------
  3 | rweasley     | $2a$10$7zCL9VNMzuWnGnA7BIsT4u68A8enr0FEM4pxvYESooCIcgrQkRD/O | f     | active | f
  1 | root         | $2a$10$xNk4uLy4oy3YE66EkJqzreUqCaV/udoNyhv6xLC6QzxK8TrdWOQaG | t     | active | f
  6 | ssnape       | $2a$10$8ZSV08sItd.lQ1uiUGJJyuWpOKzeXhdmo8lDf8JE2OmX5tQ9DnA5e | f     | active | f
  2 | hpotter      | $2a$10$HrY1lsI3u6v/sYBbBRhtc.Zq81LcNg/8cEmcrDgf/lNT4D/fFNtsa | f     | active | f
  5 | adumbledore  | $2a$10$BdEKz1CBfC2BTjYfPj1HPuDt.gU08PF6cPNn0fuL00iusfLGtO2Ge | t     | active | f
  4 | hgranger     | $2a$10$7Nr1zqIOZFVc287d.VwkSurBYihT/5g.1PMb1Hv4HgFPKCdhT5Xim | f     | active | f
(6 rows)
```

Bitbucket

Access Model

4 permission levels

- Global, Project, Repository, Branch

Global Permissions

- Bitbucket User, Project Creator, Admin, System Admin

Project Permissions

- Project Admin, Write, Read

Repo Permissions

- Admin, Write, Read

Access Token Scopes

- Repository read, Repository write, Repository admin, Project read, Project write, Project admin

API Capabilities

- REST API

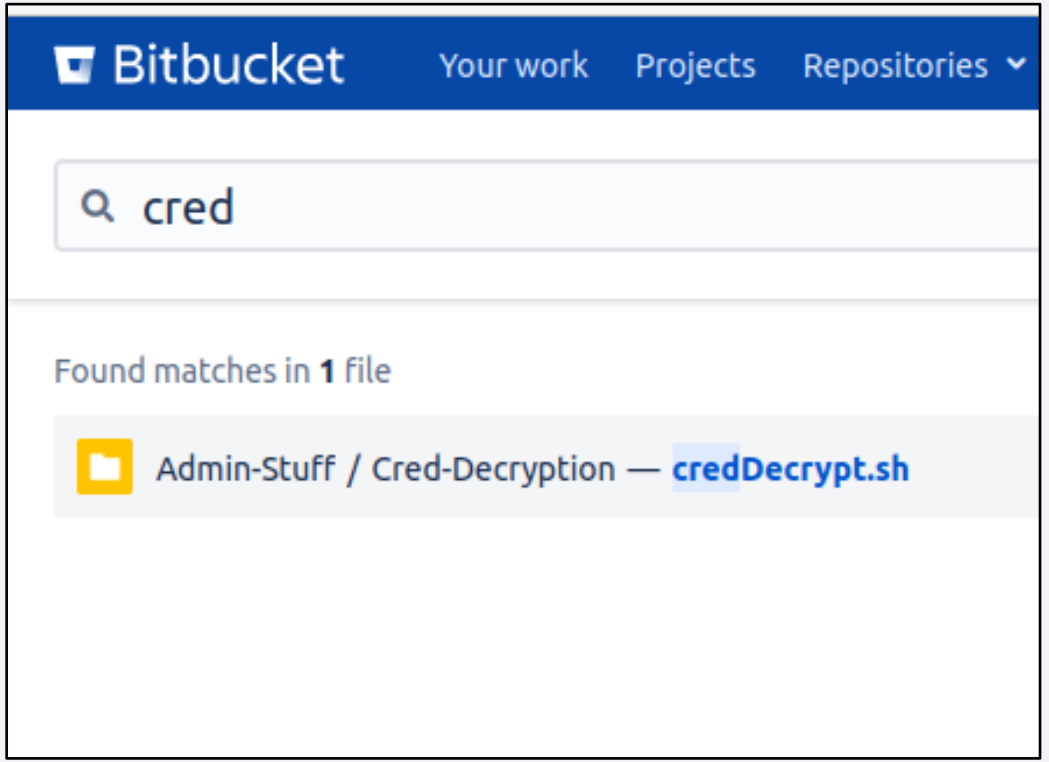
- Interact with:
  - Repositories
  - SSH Keys
  - Users
  - Admin functionality
  - And much more…

Attack Scenarios

Attack Scenario	Sub-Scenario	Admin Required?
Reconnaissance	-Repository -File -Code	No
Promoting User to Admin Role	N/A	Yes
Maintain Persistent Access	-Personal Access Token -SSH Key	No
Modifying CI/CD Pipeline	N/A	No

Reconnaissance

- Web interface or REST API
  - Repository, File, Code



Reconnaissance Logging

Bitbucket Log

- /var/log/atlassian/application-data/bitbucket/log/atlassian-bitbucket.log

Search Criteria

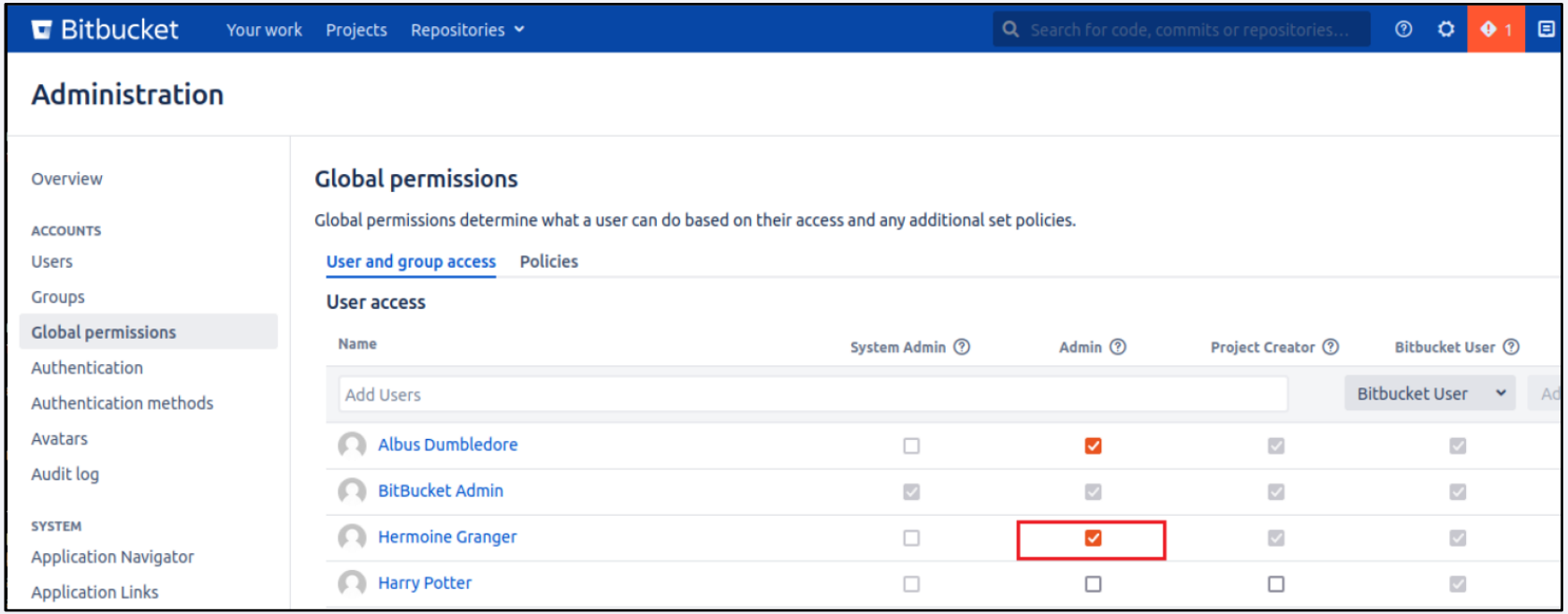
- 'post' AND 'search' AND 'query'

- Need to increase logging level

```
ket-server:~$ cat /var/atlassian/application-data/bitbucket/log/atlassi
 grep -i post | grep -i search | grep -i query
:00,327 DEBUG [http-nio-7990-exec-10] bitbucket-admin @1GXX8USx842x109x
1.54 "POST /rest/search/latest/search HTTP/1.1" c.a.b.i.s.s.DefaultSear
ch query: {
:00,328 DEBUG [http-nio-7990-exec-8] bitbucket-admin @1GXX8USx843x110x1
.54 "POST /rest/search/latest/search HTTP/1.1" c.a.b.i.s.s.DefaultSearc
h query: {
:00,512 DEBUG [http-nio-7990-exec-10] bitbucket-admin @1GXX8USx842x109x
1.54 "POST /rest/search/latest/search HTTP/1.1" c.atlassian.bitbucket.s
g: Search request execution took 225.9 ms [225 ms] for query 'api'
:00,513 DEBUG [http-nio-7990-exec-8] bitbucket-admin @1GXX8USx843x110x1
.54 "POST /rest/search/latest/search HTTP/1.1" c.atlassian.bitbucket.se
: Search request execution took 214.1 ms [214 ms] for query 'api '
:00,602 DEBUG [http-nio-7990-exec-9] bitbucket-admin @1GXX8USx843x111x2
.54 "POST /rest/search/latest/search HTTP/1.1" c.a.b.i.s.s.DefaultSearc
h query: {
:00,642 DEBUG [http-nio-7990-exec-9] bitbucket-admin @1GXX8USx843x111x2
.54 "POST /rest/search/latest/search HTTP/1.1" c.atlassian.bitbucket.se
: Search request execution took 41.36 ms [41 ms] for query 'api_key'
:02.324 DEBUG [http-nio-7990-exec-2] bitbucket-admin @1GXX8USx843x118x0
```

Promote User to Admin Role

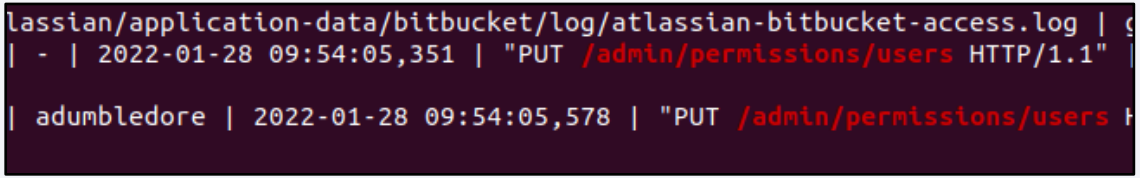
- Using admin privileges, add any user to admin



Promote User to Admin Role Logging

Access Log

- /var/atlassian/application-data/bitbucket/log/atlassian-bitbucket-access.log



Audit Log

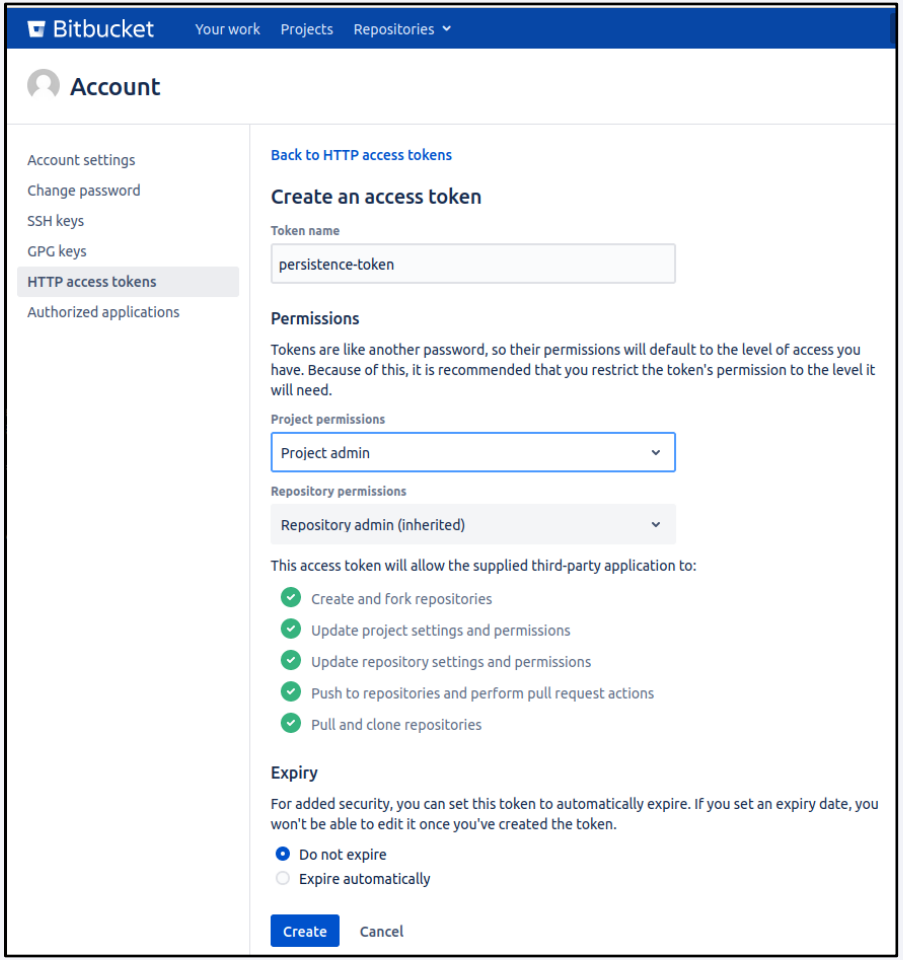
- /var/atlassian/application-data/bitbucket/log/audit/*.log

Search Criteria

- 'put' AND '/admin/permissions/users'
- 'new.permission' AND 'admin'

Maintain Persistent Access

- Personal Access Token
- SSH Key



Maintain Persistent Access Logging

Access Log

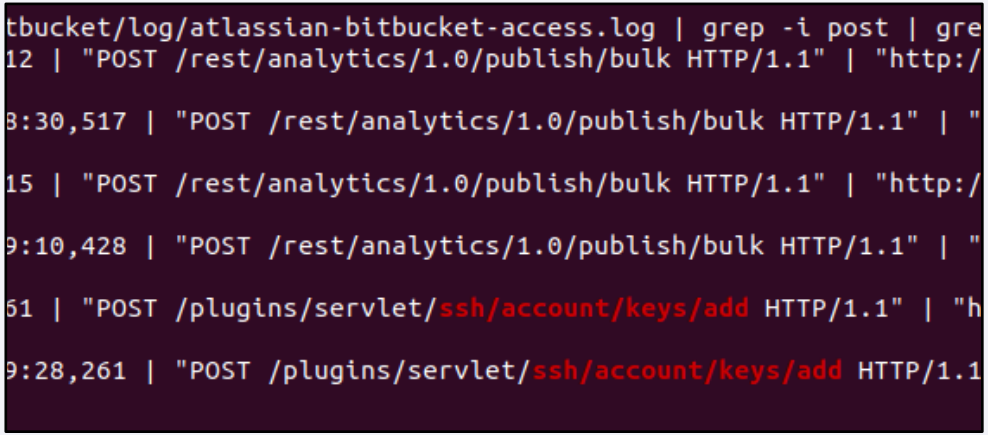
- /var/atlassian/application-data/bitbucket/log/atlassian-bitbucket-access.log

Audit Log

- /var/atlassian/application-data/bitbucket/log/audit/*.log

Search Criteria

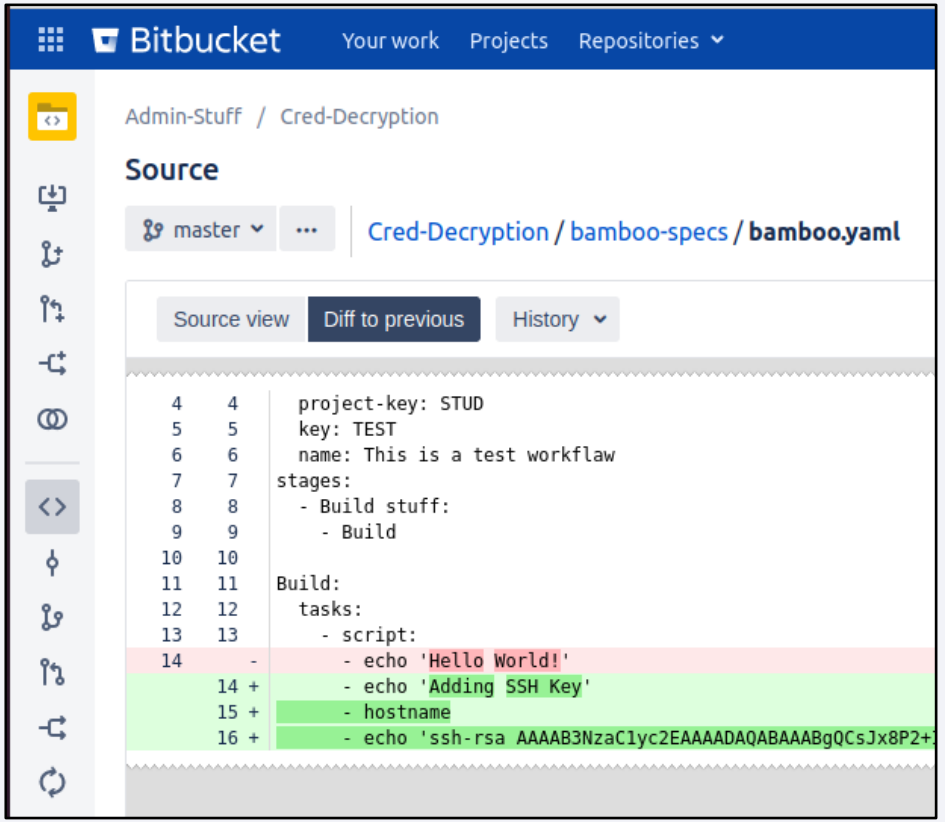
- 'put' AND '/rest/access-tokens'
- 'post' AND 'ssh/account/keys/add'
- 'personal access token created’
- 'user added ssh access key’



Modifying CI/CD Pipeline

- Discovery of CI/CD Configuration file

- Modify CI/CD Configuration file
  - Triggers pipeline to run



Modifying CI/CD Pipeline Logging

Bamboo Log

- $BAMBOO_HOME/atlassian-bamboo.log

Search Criteria

- 'change detection found'

```
cat /var/atlassian/application-data/bamboo/logs/atlassian-bamboo.log | grep -i "change detection found"
M::PlanExec:pool-16-thread-1] [ChangeDetectionListenerAction] : Change detection found 5 changes for plan STUD-TEST
M::PlanExec:pool-16-thread-3] [ChangeDetectionListenerAction] : Change detection found 1 change for plan STUD-TEST
M::PlanExec:pool-16-thread-1] [ChangeDetectionListenerAction] : Change detection found 1 change for plan STUD-TEST
```

SCMKit

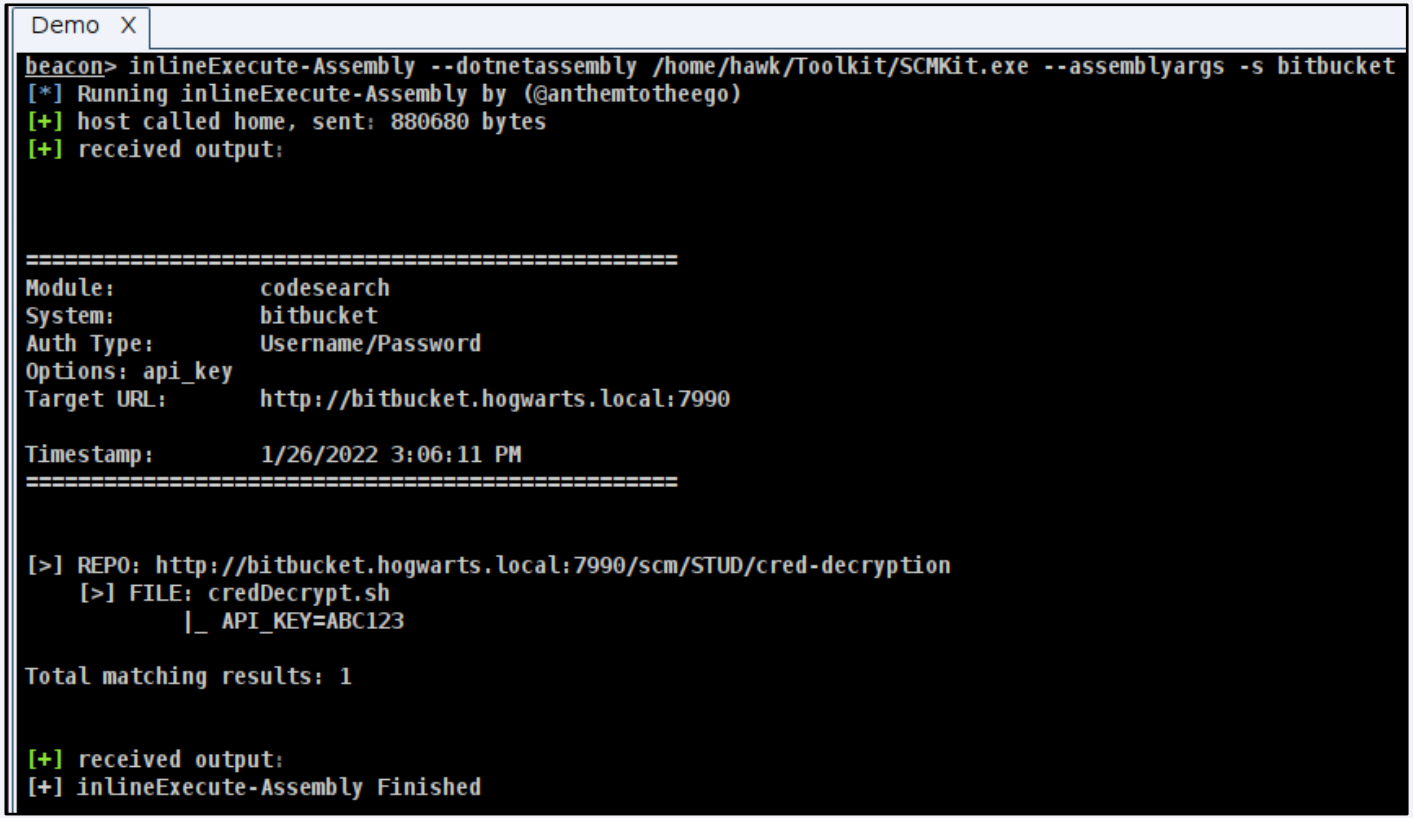
Background

- **S**ource **C**ode **M**anagement Attack Tool**kit** written in C#
  - https://github.com/xforcered/SCMKit
  - Full presentation at Black Hat USA Arsenal 2022

- Supported SCM systems:
  - GitHub Enterprise, GitLab Enterprise, Bitbucket Server

- Modules include:
  - Reconnaissance, Privilege Escalation, Persistence

Example - Reconnaissance



Example - Privilege Escalation

Demo X

```
beacon> inlineExecute-Assembly --dotnetassembly /home/hawk/Toolkit/SCMKit.exe --assemblyargs -s github -m addadmin
[*] Running inlineExecute-Assembly by (@anthemtotheego)
[+] host called home, sent: 880680 bytes
[+] received output:



================================================
Module:            addadmin
System:            github
Auth Type:         Username/Password
Options: hgranger
Target URL:        https://github-enterprise.hogwarts.local

Timestamp:         1/26/2022 3:20:38 PM
================================================

[+] SUCCESS: The user hgranger has been added to site admins


[+] received output:
[+] inlineExecute-Assembly Finished
```

Example - Persistence

```
beacon> inlineExecute-Assembly --dotnetassembly /home/hawk/Toolkit/SCMKit.exe --assemblyargs -s gitlab
[*] Running inlineExecute-Assembly by (@anthemtotheego)
[+] host called home, sent: 880669 bytes
[+] received output:



================================================
Module:           createpat
System:           gitlab
Auth Type:        API Key
Options: hgranger
Target URL:       https://gitlab.hogwarts.local

Timestamp:        1/26/2022 3:10:13 PM
================================================

   ID |         Name |                          Token
------------------------------------------------------
   61 | SCMKIT-oHQpZ |          G4RzYez1_6Qzr1n48R_U

[+] SUCCESS: The hgranger user personal access token was successfully added.



[+] received output:
[+] inlineExecute-Assembly Finished
```

Demos

Demos

Demo 1: Software Supply Chain Attack - Repository Takeover on GitHub Enterprise

Demo 2: Lateral Movement from GitLab Enterprise to Artifactory

Demo 3: Lateral Movement from Bitbucket to Jenkins

Defensive Considerations

SCMKit

- Static signatures in YARA rule file in SCMKit repo

- Static user agent string
  - `SCMKIT-5dc493ada400c79dd318abbe770dac7c`

- All access token and SSH key names created in SCM systems prepended with “SCMKIT-”

GitHub Enterprise – Important Logs

Log Name	Location
Audit Log	`/var/log/github-audit.log*`
Management Log	`/var/log/enterprise-manage/unicorn.log*`
HAProxy Log	`/var/log/haproxy.log`

GitHub Enterprise – Log Filters

Attack Scenario	Log Name	Search Filter
Reconnaissance	HAProxy Log	('/search' OR '/api/v3/search') AND 'http'
Repository Takeover	Audit Log	'action:repo.staff_unlock'
User Impersonation	Audit Log	'action:staff.fake_login' OR 'action:oauth_access.create' OR 'action:oauth_authorization.create'
Promoting User to Site Admin	Audit Log	'action:user.promote' OR 'action:business.add_admin'
Maintaining Persistent Access	Audit Log	'action:oauth_access.create' OR 'action:oauth_authorization.create' OR 'action:public_key.create' OR 'action:public_key.verify'
Management Console Access	Management Log	'authorized-keys' AND 'post'

GitLab Enterprise – Important Logs

Log Name	Location
Application Log	/var/log/gitlab/gitlab-rails/application.log /var/log/gitlab/gitlab-rails/application_json.log
Production Log	/var/log/gitlab/gitlab-rails/production_json.log /var/log/gitlab/gitlab-rails/production.log
API Log	/var/log/gitlab/gitlab-rails/api_json.log
Web Log	/var/log/gitlab/nginx/gitlab_access.log

GitLab Enterprise – Log Filters

Attack Scenario	Log Name	Search Filter
Reconnaissance	Production Log	'get' AND '/search?search' 'get' AND '/search'
	API Log	'get' AND ('/search'| OR 'repository/tree')
	Web Log	'search'
User Impersonation	Application Log	'has started impersonating'
	Production Log	'impersonate' 'post' AND 'impersonation_tokens'
	API Log	'impersonation_tokens'
Promoting User to Admin Role	Production Log	'patch' AND 'admin/users'
	API Log	'put' AND '"key":"admin","value":"true"'
Maintaining Persistent Access	Production Log	'post' AND 'personal_access_tokens' 'post' AND 'profile/keys'
	API Log	'post' AND 'personal_access_tokens' 'post' AND 'user/keys'
Modifying CI/CD Pipeline	Production Log	'post' AND '/api/graphql' AND '.gitlab-ci.yml' AND 'update'

Bitbucket – Important Logs

Log Name	Location
Access Log	`/var/atlassian/application-data/bitbucket/log/atlassian-bitbucket-access.log`
Audit Log	`/var/atlassian/application-data/bitbucket/log/audit/*.log`
Bitbucket Log	`/var/atlassian/application-data/bitbucket/log/atlassian-bitbucket.log`
Bamboo Log	`$BAMBOO_HOME/atlassian-bamboo.log`

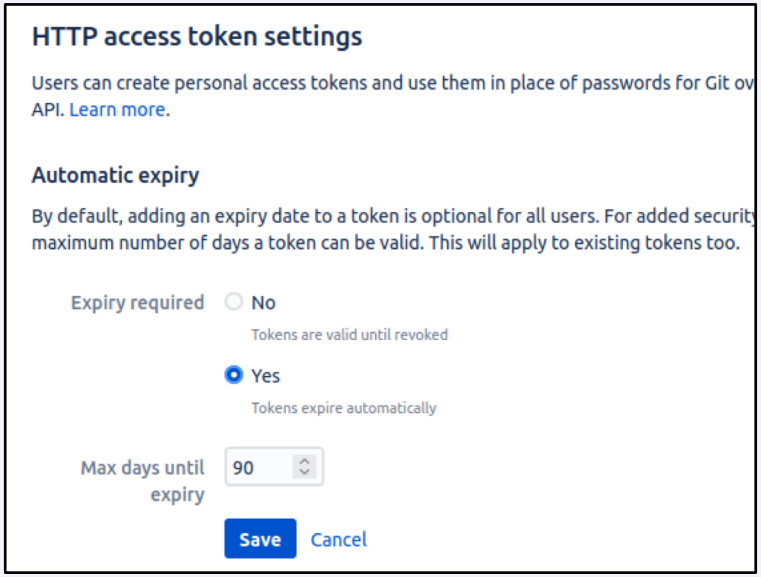
Bitbucket – Log Filters

Attack Scenario	Log Name	Search Filter
Reconnaissance	Bitbucket Log	'post' AND 'search' AND 'query'
Promoting User to Site Admin	Access Log Audit Log	'put' AND '/admin/permissions/users' 'new.permission' AND 'admin'
Maintaining Persistent Access	Access Log Audit Log	'put' AND '/rest/access-tokens' 'post' AND 'ssh/account/keys/add' 'personal access token created' 'user added ssh access key'
Modifying CI/CD Pipeline	Bamboo Log	'change detection found'

SCM System Configuration Guidance

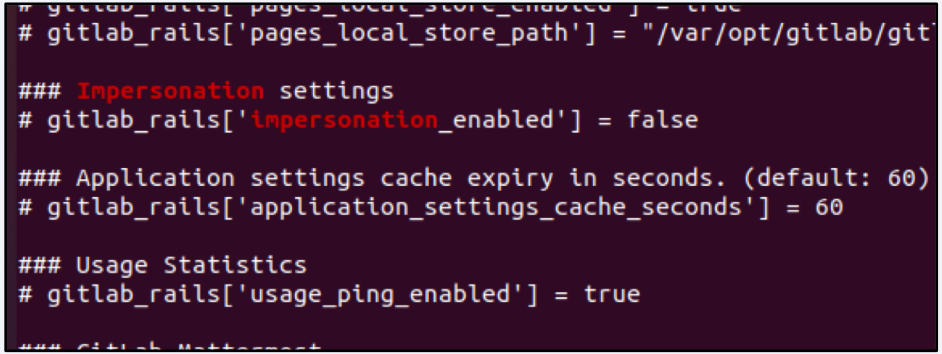
Personal Access Tokens and SSH Keys

- Set automatic expiration date
- Do not allow creation with no expiration date



Access and Authorization

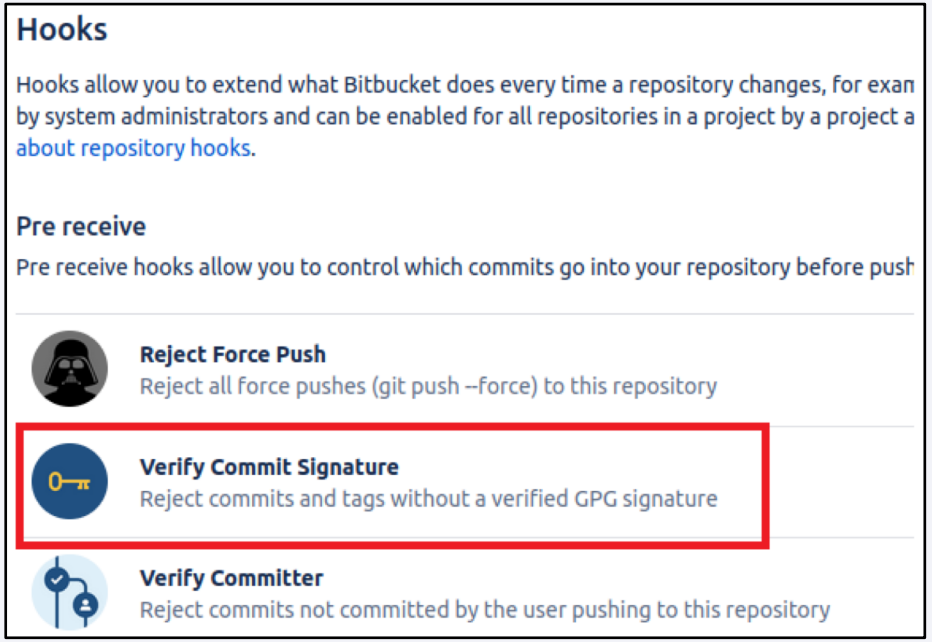
- Limit the number of admins
- Enable multi-factor authentication
- Disable user impersonation



SCM System Configuration Guidance

Repository Access and Code Commits

- Policy of least privilege
- Delete code branches in sufficient time
- Require approver(s) for commits
- Require signed commits



Logging

- Increase logging level where applicable
- Forward important logs to SIEM

Conclusion

Conclusion

- SCM systems contain some of most sensitive information in organizations
- Compromise of SCM system can lead to compromise of multiple organizations
- SCM systems need more visibility and research from information security community

Acknowledgements

Thank You to the below people for feedback and support on this research

- Chris Thompson (@retBandit)
- Daniel Crowley (@dan_crowley)
- Dimitry Snezhkov(@Op_nomad)
- Patrick Fussell (@capt_red_beardz)
- Ruben Boonen (@FuzzySec)

Questions?

Twitter: @h4wkst3r 

Discord: @h4wkst3r#9627 

Blog Post:

https://securityintelligence.com/posts/abusing-source-code-management-systems

Whitepaper:

https://www.ibm.com/downloads/cas/OG6KNX1E


IBM

Appendix - References

- https://www.cisa.gov/publication/software-supply-chain-attacks
- https://github.com/enterprise
- https://about.gitlab.com/enterprise/
- https://bitbucket.org/product/
- https://www.redhat.com/architect/devops-cicd
- https://medium.com/aws-cyber-range/secdevops-101-strengthen-the-basics-20f57197aa1c
- https://devops.com/the-basics-devsecops-adoption
- https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/
- https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor
- https://opensource.googleblog.com/2021/10/protect-your-open-source-project-from-supply-chain-attacks.html
- https://www.jenkins.io/
- https://www.jenkins.io/doc/book/pipeline/jenkinsfile/

Appendix - References

- https://www.jenkins.io/doc/book/pipeline/
- https://www.jenkins.io/doc/book/using/remote-access-api/
- https://docs.gitlab.com/runner/
- https://docs.gitlab.com/ee/api/runners.html
- https://docs.gitlab.com/ee/ci/yaml/
- https://docs.github.com/en/enterprise-server@3.3/get-started/quickstart/github-glossary
- https://docs.github.com/en/enterprise-server@3.3/admin/user-management/managing-users-in-your-enterprise/roles-in-an-enterprise
- https://docs.github.com/en/enterprise-server@3.3/organizations/managing-peoples-access-to-your-organization-with-roles/roles-in-an-organization
- https://docs.github.com/en/enterprise-server@3.3/organizations/managing-access-to-your-organizations-repositories/repository-roles-for-an-organization
- https://docs.github.com/en/developers/apps/building-oauth-apps/scopes-for-oauth-apps#available-scopes
- https://docs.github.com/en/enterprise-server@3.0/rest/guides/getting-started-with-the-rest-api

Appendix - References

- https://docs.github.com/en/enterprise-server@3.3/rest/reference/search#search-repositories
- https://docs.github.com/en/enterprise-server@3.3/rest/reference/search#search-commits
- https://docs.github.com/en/enterprise-server@3.3/rest/reference/search#search-code
- https://docs.github.com/en/enterprise-server@3.3/rest/reference/enterprise-admin#create-an-impersonation-oauth-token
- https://docs.github.com/en/enterprise-server@3.3/rest/reference/enterprise-admin#promote-a-user-to-be-a-site-administrator
- https://docs.github.com/en/enterprise-server@3.3/rest/reference/users#create-a-public-ssh-key-for-the-authenticated-user
- https://docs.github.com/en/enterprise-server@3.0/admin/configuration/configuring-your-enterprise/command-line-utilities
- https://docs.gitlab.com/ee/user/index.html
- https://docs.gitlab.com/ee/user/permissions.html#project-members-permissions
- https://docs.gitlab.com/ee/user/permissions.html#group-members-permissions

Appendix - References

- https://docs.gitlab.com/ee/user/permissions.html#gitlab-cicd-permissions
- https://docs.gitlab.com/ee/user/permissions.html#job-permissions
- https://docs.gitlab.com/ee/user/profile/personal_access_tokens.html#personal-access-token-scopes
- https://docs.gitlab.com/ee/api/index.html
- https://docs.gitlab.com/ee/api/search.html#scope-projects
- https://docs.gitlab.com/ee/user/search/advanced_search.html
- https://docs.gitlab.com/ee/api/repositories.html#list-repository-tree
- https://docs.gitlab.com/ee/api/search.html#scope-blobs-premium-2
- https://docs.gitlab.com/ee/administration/audit_events.html#impersonation-data
- https://docs.gitlab.com/ee/api/users.html#create-an-impersonation-token
- https://docs.gitlab.com/ee/api/users.html#user-modification
- https://docs.gitlab.com/ee/api/users.html#create-a-personal-access-token

Appendix - References

- https://docs.gitlab.com/ee/api/users.html#add-ssh-key
- https://www.atlassian.com/software/bitbucket/enterprise
- https://bitbucket.org/product/guides/getting-started/overview#key-terms-to-know
- https://confluence.atlassian.com/bitbucketserverkb/4-levels-of-bitbucket-server-permissions-779171636.html
- https://confluence.atlassian.com/bitbucketserver/global-permissions-776640369.html
- https://confluence.atlassian.com/bitbucketserver/using-project-permissions-776639801.html
- https://confluence.atlassian.com/bitbucketserver/using-repository-permissions-776639771.html
- https://confluence.atlassian.com/bitbucketserver/using-branch-permissions-776639807.html
- https://confluence.atlassian.com/bitbucketserver/http-access-tokens-939515499.html
- https://developer.atlassian.com/server/bitbucket/reference/rest-api/
- https://docs.atlassian.com/bitbucket-server/rest/7.20.0/bitbucket-rest.html#idp450
- https://docs.atlassian.com/bitbucket-server/rest/4.5.1/bitbucket-rest.html#idp3716336

Appendix - References

- https://docs.atlassian.com/bitbucket-server/rest/7.20.0/bitbucket-access-tokens-rest.html
- https://docs.atlassian.com/bitbucket-server/rest/7.20.0/bitbucket-ssh-rest.html
- https://www.atlassian.com/software/bamboo
- https://docs.atlassian.com/bamboo-specs-docs/8.1.2/specs.html?yaml#
- https://docs.atlassian.com/bamboo-specs-docs/8.1.2/specs.html?java#
- https://github.com/xforcered/SCMKit
- https://krebsonsecurity.com/2022/04/leaked-chats-show-lapsus-stole-t-mobile-source-code/
- https://threatpost.com/microsoft-lapsus-compromised-one-employees-account/179048/
- https://techcrunch.com/2022/03/30/lapsus-globant-breach/
- https://www.bleepingcomputer.com/news/security/hackers-leak-190gb-of-alleged-samsung-data-source-code/
- https://securityintelligence.com/posts/abusing-source-code-management-systems
- https://www.ibm.com/downloads/cas/OG6KNX1E