

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

- SCM systems used during “Build” phase

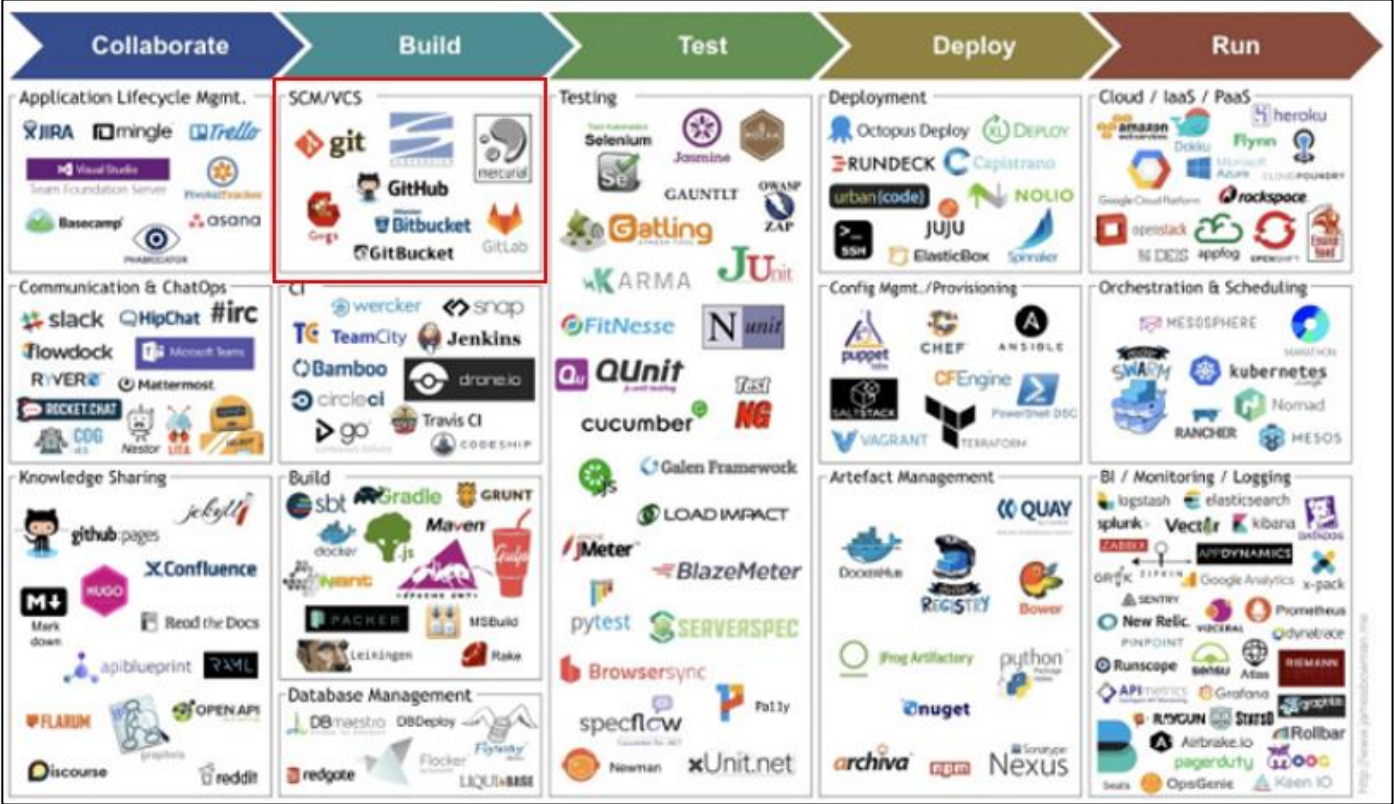


Image: <https://medium.com/aws-cyber-range/secdevops-101-strengthen-the-basics-20f57197aa1c>

Software Supply Chain Attacks

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

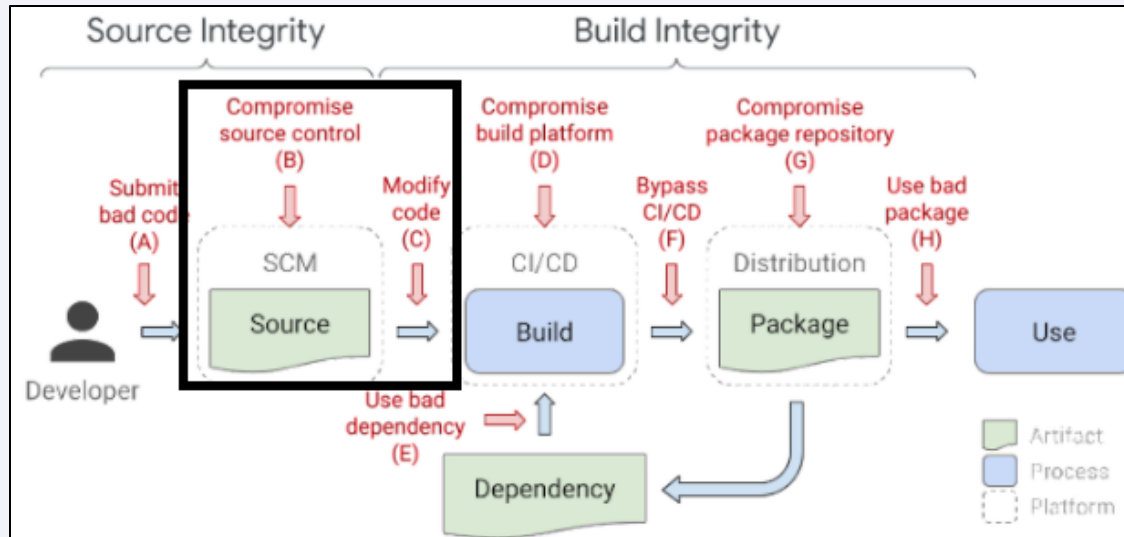


Image: <https://opensource.googleblog.com/2021/10/protect-your-open-source-project-from-supply-chain-attacks.html>

Lateral Movement to other DevOps Systems

SCM Systems

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

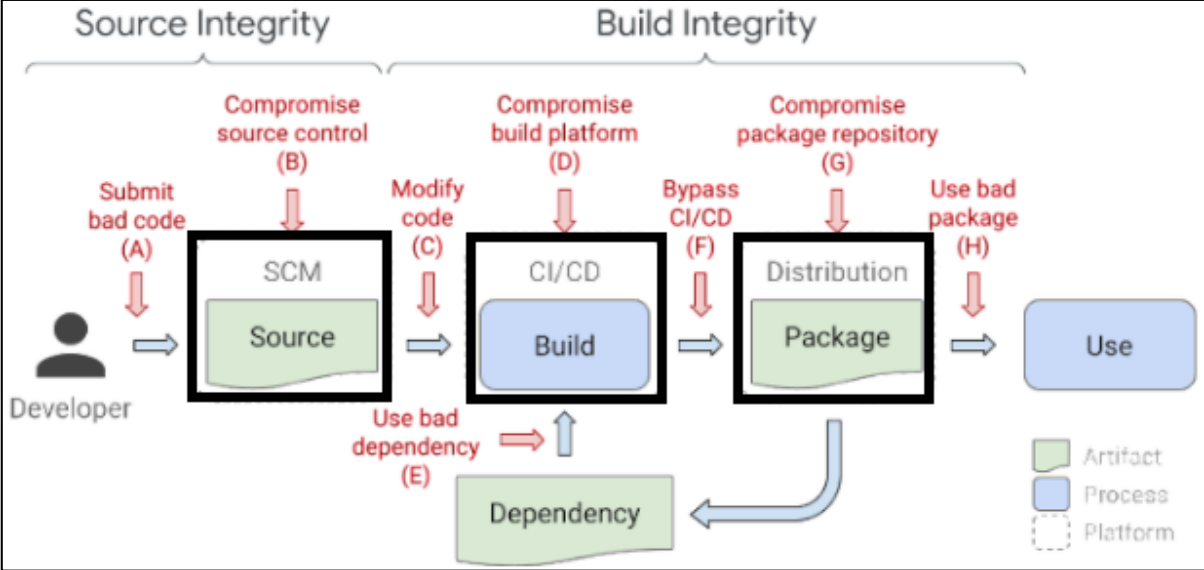


Image: <https://opensource.googleblog.com/2021/10/protect-your-open-source-project-from-supply-chain-attacks.html>

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

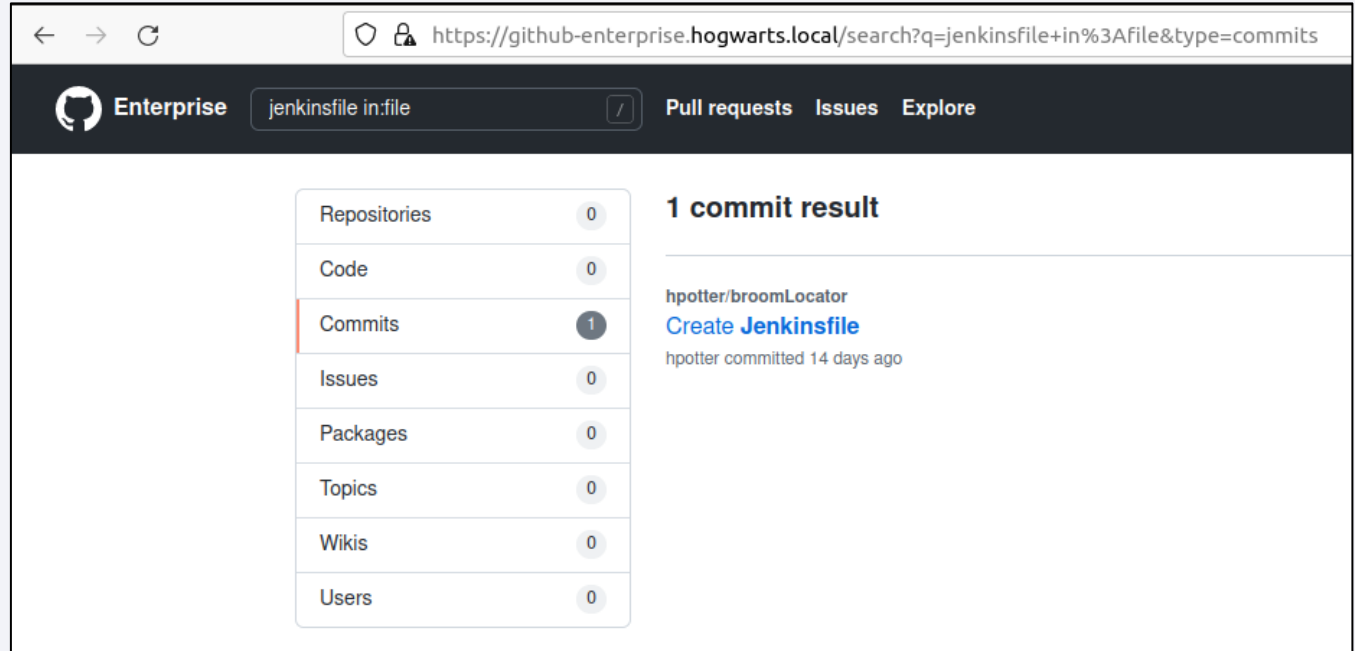
- REST API
- Interact with:
 - Repositories
 - SSH Keys
 - Users
 - Admin functionality
 - And much more...

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

- Interact with web interface or REST API
- Repository, File, Code



The screenshot shows a web browser window displaying the GitHub Enterprise search interface. The address bar shows the URL: `https://github-enterprise.hogwarts.local/search?q=jenkinsfile+in%3Afile&type=commits`. The search bar contains the query `jenkinsfile in:file`. The search results are categorized by type, with 'Commits' showing 1 result. The result is for the repository `hpotter/broomLocator` and is titled `Create Jenkinsfile`, committed 14 days ago.

Category	Count
Repositories	0
Code	0
Commits	1
Issues	0
Packages	0
Topics	0
Wikis	0
Users	0

1 commit result

`hpotter/broomLocator`
[Create Jenkinsfile](#)
hpotter committed 14 days ago

Reconnaissance Logging

HAProxy Log

- /var/log/haproxy.log

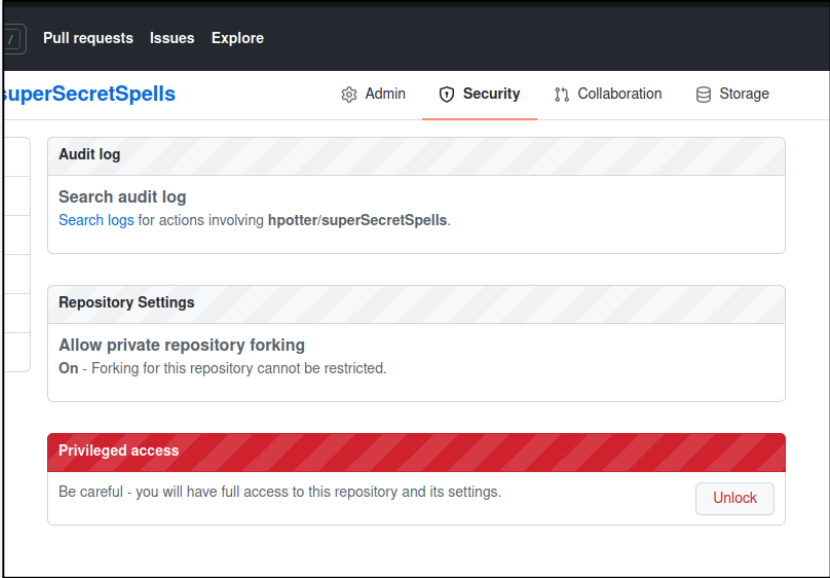
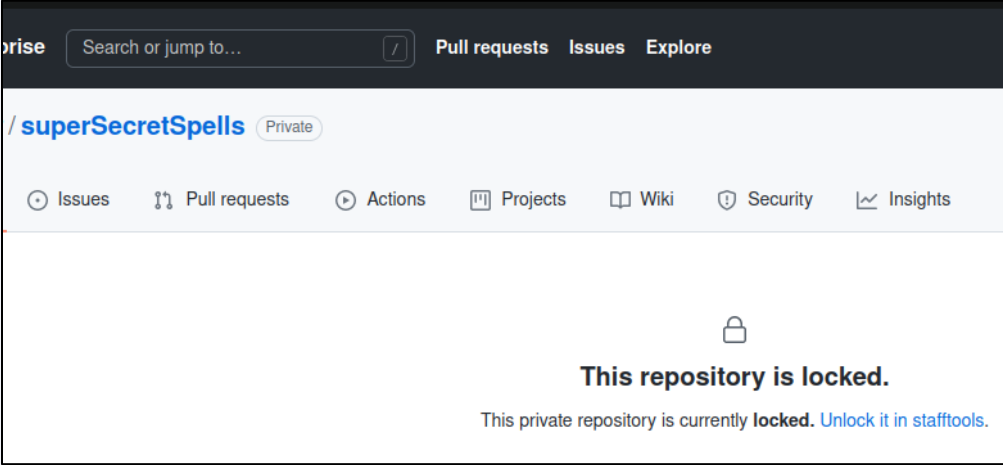
Search Criteria

- ('/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



Repository Takeover Logging

Audit Log

- /var/log/github-audit.log

Search Criteria

- action:repo.staff_unlock

The screenshot displays the GitHub Audit Log interface. On the left is a navigation menu with options like 'Management console', 'Audit log', 'Explore', 'Reports', 'Indexing', 'Repository networks', 'File storage', 'Reserved logins', 'Advanced Security Committers', 'Retired namespaces', 'Enterprise overview', 'Repositories', 'Billing', 'Product catalog', 'Invite user', 'All users', 'Site admins', 'Dormant users', and 'Suspended users'. The 'Audit log' option is selected. The main content area shows a search query 'action:repo.staff_unlock' and a search button. Below the search bar, there are links for 'Advanced Search' and 'Newer Older'. A section titled 'Copy all log metadata for internal use' provides instructions on copying log entries as JSON. The main section is titled 'Logs for action:repo.staff_unlock' and displays a single log entry. The entry details are as follows:

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/
repo	hpotter/superSecretSpells
repo_id	1
request_category	other
request_id	5fad2fd5-eecf-4cd4-841d-6041dde8b571
server_id	9770622b-4f35-42e8-9963-c158f1306674

User Impersonation

- Impersonate User Login
- Impersonation Token

The screenshot shows the GitHub Site Admin interface for user 'hpotter'. The page is titled 'User information' and shows the user is 'Active'. A left-hand navigation menu includes: Overview, Admin, Emails, Avatars, Feature & Beta Enrollments, Followed users, Search, Database, Retired namespaces, Scheduled Reminders, and Profile. The main content area displays user details:

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	×

Below the user information is an 'Activity feed' section with buttons for 'Clear public activity' and 'Clear all activity'. Underneath is a 'Staff notes' section with an 'Add note' button and a message: 'There are no staff notes on this account.' At the bottom, a red 'Danger Zone' banner contains an 'Impersonate' button with a sub-button '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

Reserved logins	Logs for action:oauth_access.create OR action:oauth_authorization.create
Advanced Security Committers	
Retired namespaces	
Enterprise overview	
Repositories	
Billing	
Product catalog	
Invite user	
All users	
Site admins	
Dormant users	
Suspended users	

oauth_authorization.create
OAuth application (GitHub Site Administrator)
Performed by **adumbledore** from **192.168.1.54**
Targeting user **hpotter** ...

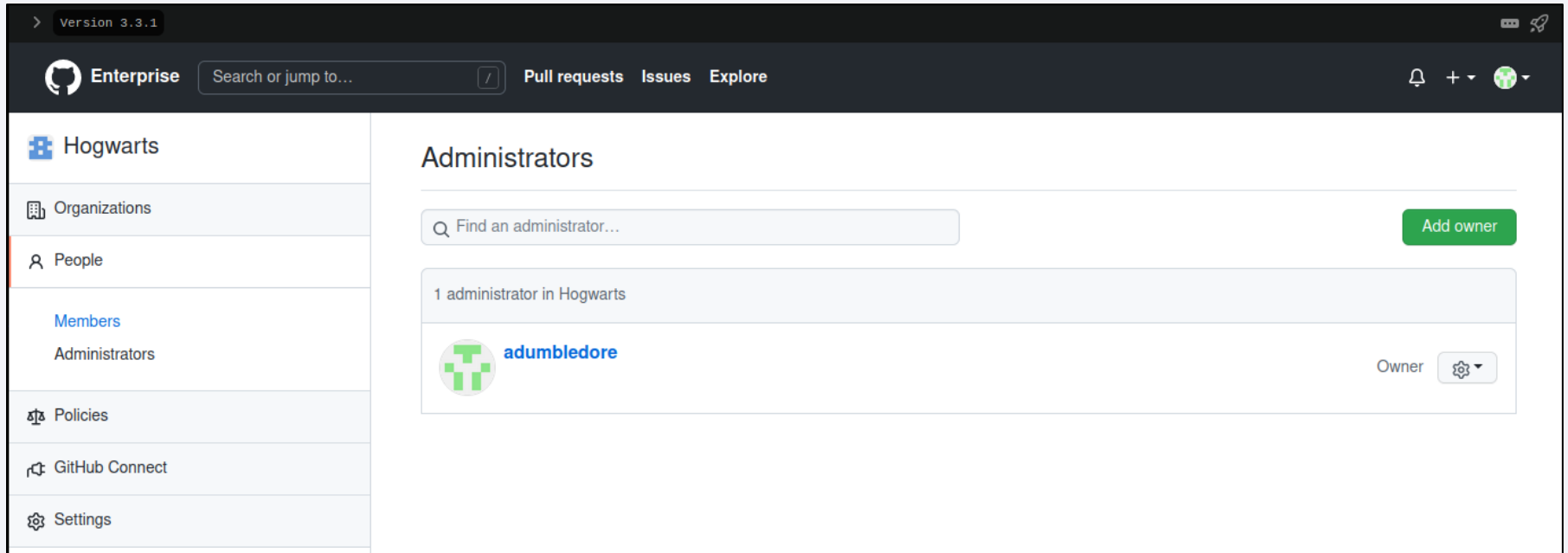
oauth_access.create
OAuth application (GitHub Site Administrator)
Performed by **adumbledore** from **192.168.1.54**
Targeting user **hpotter** ...

[Copy entry cURL](#)

```
accessible_org_ids blank
action          oauth_access.create
actor           adumbledore
actor_id        4
actor_ip        192.168.1.54
actor_location  blank
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    e7KP7cn89puTnt6XMt1WmT85Un59eFzllGRGTPx+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       192.168.1.54
```


Promoting User to Site Admin

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



The screenshot shows the GitHub Enterprise interface for the 'Hogwarts' organization. The top navigation bar includes the GitHub logo, 'Enterprise', a search bar, and links for 'Pull requests', 'Issues', and 'Explore'. The left sidebar contains navigation options: 'Hogwarts', 'Organizations', 'People', 'Members', 'Administrators', 'Policies', 'GitHub Connect', and 'Settings'. The main content area is titled 'Administrators' and features a search bar with the placeholder text 'Find an administrator...'. A green 'Add owner' button is located to the right of the search bar. Below the search bar, a box indicates '1 administrator in Hogwarts'. The administrator listed is 'adumbledore', represented by a green and blue icon. To the right of the name, the role is 'Owner' with a settings gear icon.

Promoting User to Site Admin Logging

Audit Log

- `/var/log/github-audit.log`

Search Criteria

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

The screenshot displays the GitHub Site Admin interface. On the left is a navigation sidebar with the following items: Site admin, Search, Management console, Audit log (highlighted), Explore, Reports, Indexing, Repository networks, File storage, Reserved logins, Advanced Security Committers, Retired namespaces, Enterprise overview, Repositories, Billing, Product catalog, Invite user, and All users. The main content area is titled 'Audit log' and features a search bar with the query 'action:user.promote OR action:business.add_admin' and a 'Search' button. Below the search bar is an 'Advanced Search' link and navigation links for 'Newer' and 'Older'. A section titled 'Copy all log metadata for internal use' provides instructions on copying log entry metadata to a clipboard as JSON, noting that the data is sanitized. Below this is a heading 'Logs for action:user.promote OR action:business.a' followed by three log entries:

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

Maintain Persistent Access

- Personal Access Token
- Impersonation Token
- SSH Key

The screenshot shows the 'Developer settings' page in GitHub. On the left, a sidebar menu has 'Personal access tokens' selected. The main content area is titled 'New personal access token'. It includes a text input for the token name (filled with 'persistence-token'), a dropdown for expiration (set to 'No expiration'), and a list of scopes. The 'repo' scope is checked, and its sub-scopes are also checked. The 'workflow' and 'write:packages' scopes are unchecked.

Settings / Developer settings

New personal access token

Personal access tokens function like ordinary OAuth access tokens. They can be used in applications 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 your account 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 checked="" type="checkbox"/> repo:status	Access commit status
<input checked="" type="checkbox"/> repo_deployment	Access deployment status
<input checked="" type="checkbox"/> public_repo	Access public repositories
<input checked="" type="checkbox"/> repo:invite	Access repository invitations
<input checked="" 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 displays the GitHub Audit Log interface. On the left is a navigation sidebar with the following items: Site admin, Search, Management console, Audit log, Explore, Reports, Indexing, Repository networks, File storage, Reserved logins, Advanced Security Committers, Retired namespaces, Enterprise overview, Repositories, Billing, Product catalog, Invite user, All users, Site admins, Dormant users, and Suspended users. The main content area is titled 'Audit log' and features a search bar with the query 'action:oauth_access.create OR action:oauth_authorization.create'. Below the search bar are links for 'Advanced Search', 'Newer', and 'Older'. A section titled 'Copy all log metadata for internal use' provides instructions on copying log data. The search results show two entries: 'oauth_authorization.create' and 'oauth_access.create', both performed by 'hpotter' from IP '192.168.1.54'. A detailed JSON metadata view for the 'oauth_access.create' entry is shown at the bottom, with a 'Copy' button.

Site admin

Search

Management console

Audit log

Explore

Reports

Indexing

Repository networks

File storage

Reserved logins

Advanced Security Committers

Retired namespaces

Enterprise overview

Repositories

Billing

Product catalog

Invite user

All users

Site admins

Dormant users

Suspended users

Audit log

Query

action:oauth_access.create OR action:oauth_authorization.create Search

Advanced Search

Newer Older

Copy all log metadata for internal use

Copy the metadata of all displayed log entries to your clipboard as JSON-formatted data. Data that is copied has been sanitized of sensitive data but may include actions the user can see. Share with caution.

Logs for action:oauth_access.create OR action:oauth_authorization.create

oauth_authorization.create
Personal access token (persistence-token)
Performed by **hpotter** from **192.168.1.54**
Targeting user **hpotter**

oauth_access.create
Personal access token (persistence-token)
Performed by **hpotter** from **192.168.1.54**
Targeting user **hpotter**

accessible_org_ids blank

action oauth_access.create

actor hpotter

actor_id 6

actor_ip 192.168.1.54

actor_location blank

actor_session 16

application_id 0

application_name persistence-token

category_type Other

client_id 2060490046.1643228505

Copy

Management Console Access

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

The screenshot displays the 'Settings' page of the IBM Security Management Console. The page has a dark theme. On the left is a vertical navigation menu with options: Settings, Password, SSH access, Hostname, Time, Authentication, Privacy, Pages, Email, Monitoring, Rate limiting, Applications, Actions, Packages, Security, and Mobile. The 'Password' option is currently selected. The main content area is titled 'Settings' and includes a warning: 'Your instance will restart automatically when you save these settings. Please wait a few minutes for the changes to take effect.' Below this, there are two sections: 'Change password' and 'SSH access'. The 'Change password' section explains that the password is used for login and as an API key, and provides a link to the password settings page. The 'SSH access' section explains that it grants limited SSH access and shows a terminal command: `ssh -p 122 admin@github-enterprise.hogwarts.local`. Below this, there is a section for 'Authorized SSH keys' which currently shows no keys. At the bottom of this section is an 'Add new SSH key' button. A text area below the button contains a sample SSH key: `ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCsJx8P2+IGHpcak0IMX57g0t+tDK5nBIS9cVISnO8JpJQ8JKSnKNSjodEuKL5y3+4qahM4owbqlcjmM17Kr0AqESn0GGmBB5kS9FECbutsQuYBcf1dDdxXevMiYjuoGyYLUmvR8z3g6lqpMXiiZU23pNAWV6fvxHYa7OK/U1`. An 'Add key' button is located at the bottom right of the text area.

Settings

Your instance will restart automatically when you save these settings. Please wait a few minutes for the changes to take effect. ⓘ

- Settings
- Password**
- SSH access
- Hostname
- Time
- Authentication
- Privacy
- Pages
- Email
- Monitoring
- Rate limiting
- Applications
- Actions
- Packages
- Security
- Mobile

Change password

This password is how you login to the Enterprise Management Console and also serves as your API key. You can change it by going to the [password settings page](#). SSH administrative access uses authorized SSH keys you've added instead of this password.

SSH access ⓘ

This grants limited SSH access to the appliance to perform specific operations. You can access this appliance via `ssh -p 122 admin@github-enterprise.hogwarts.local`.

Authorized SSH keys

There are no authorized keys in your instance.

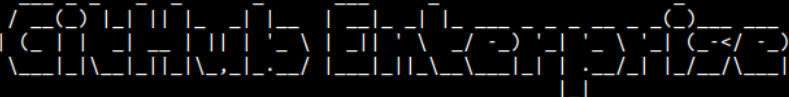
Add new SSH key

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGCsJx8P2+IGHpcak0IMX57g0t+tDK5nBIS9cVISnO8JpJQ8J
KSnKNSjodEuKL5y3+4qahM4owbqlcjmM17Kr0AqESn0GGmBB5kS9FECbutsQuYBcf1dDdxXevMiYju
oGyYLUmvR8z3g6lqpMXiiZU23pNAWV6fvxHYa7OK/U1
```

Add 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

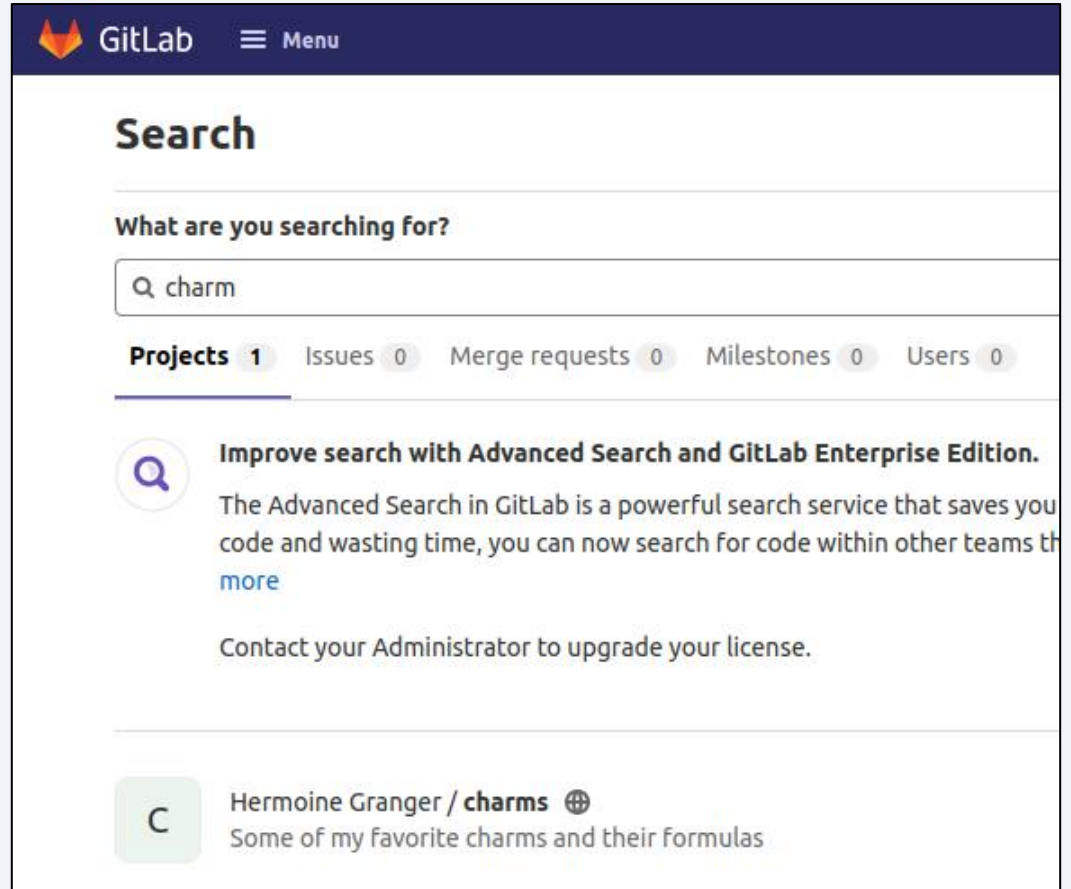
- REST API
- Interact with:
 - Repositories
 - SSH Keys
 - Users
 - Admin functionality
 - And much more...

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

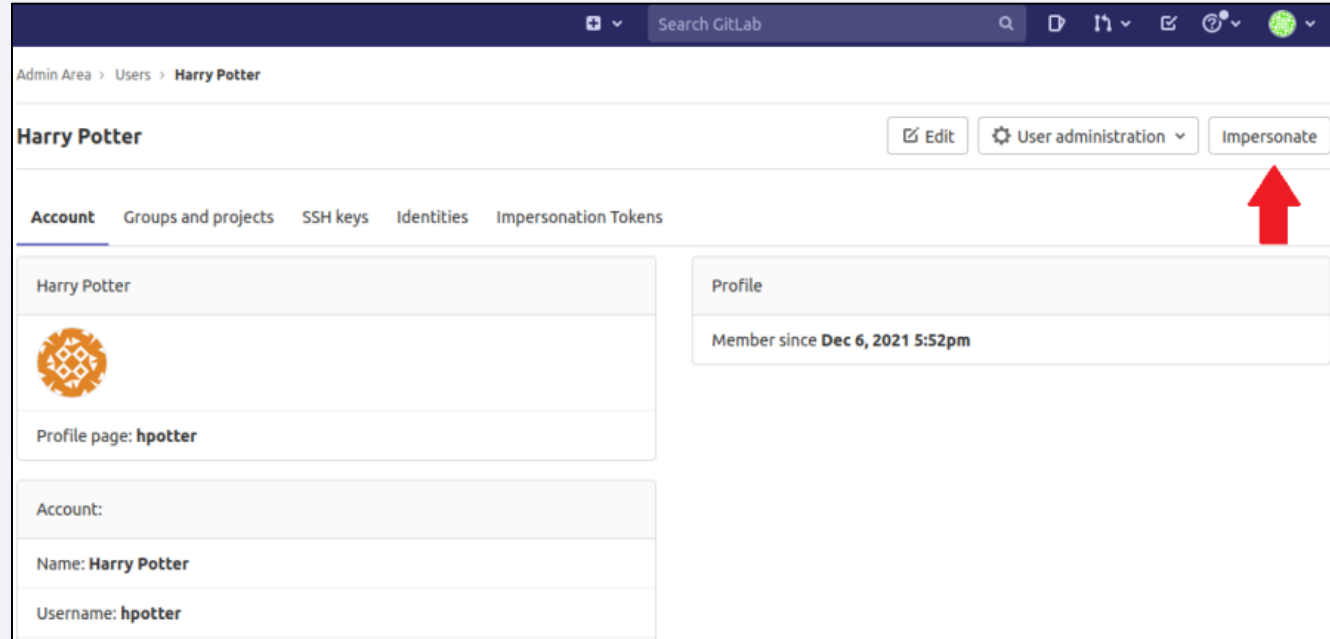
- Interact with web interface or REST API
 - Repository, File, Code



The screenshot displays the GitLab search page. At the top, the GitLab logo and a 'Menu' button are visible. The main heading is 'Search'. Below it, a search bar contains the text 'charm'. A summary row shows 'Projects 1', 'Issues 0', 'Merge requests 0', 'Milestones 0', and 'Users 0'. The first search result is a promotional message: 'Improve search with Advanced Search and GitLab Enterprise Edition.' It includes a search icon, a description of the service, and a link to 'more'. Below this is a call to action: 'Contact your Administrator to upgrade your license.' The second search result is a repository entry for 'Hermoine Granger / charms', featuring a green profile icon with the letter 'C' and a globe icon.

User Impersonation

- Impersonate User Login
- Impersonation Token



The screenshot displays the GitLab Admin Area for a user named Harry Potter. The breadcrumb navigation shows 'Admin Area > Users > Harry Potter'. The user's name 'Harry Potter' is prominently displayed at the top, with 'Edit', 'User administration', and 'Impersonate' buttons to its right. A red arrow points to the 'Impersonate' button. Below the name, there are tabs for 'Account', 'Groups and projects', 'SSH keys', 'Identities', and 'Impersonation Tokens'. The 'Account' tab is active, showing the user's profile information, including a profile picture, profile page link, account name, and username.

Admin Area > Users > Harry Potter

Harry Potter [Edit](#) [User administration](#) [Impersonate](#)

Account Groups and projects SSH keys Identities Impersonation Tokens

Harry Potter

Profile

Member since Dec 6, 2021 5:52pm

Profile page: [hpotter](#)

Account:

Name: Harry Potter

Username: hpotter

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

Account

Name
* required

Username
* required

Email
* required

Password

Password

Password confirmation

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

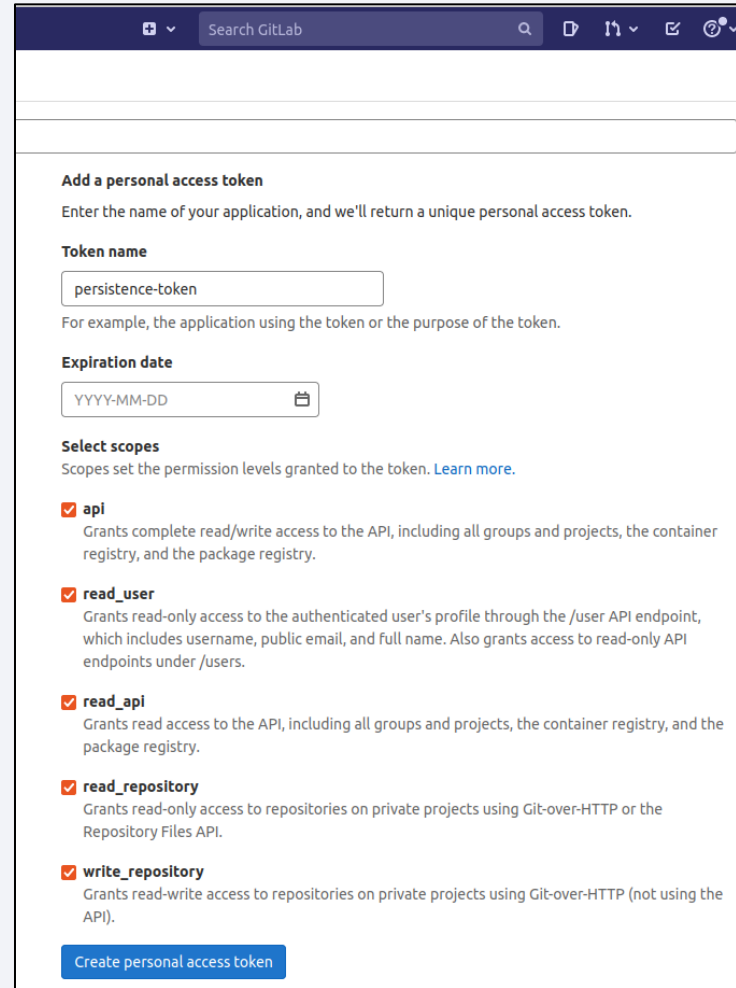
```
/gitlab-rails/api_json.log | grep -i PUT | grep -i '"key":"admin","value":"true"
ity":"INFO","duration_s":0.07148,"db_duration_s":0.01323,"view_duration_s":0.058
"/api/:version/users/:id","user_id":5,"username":"adumbledore","queue_duration_s
":442,"redis_cache_write_bytes":225,"redis_shared_state_calls":2,"redis_shared_s
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' page in the GitLab web interface. The browser's address bar shows 'Search GitLab'. The page content includes:

- Add a personal access token**
Enter the name of your application, and we'll return a unique personal access token.
- Token name**
A text input field containing 'persistence-token'.
- For example, the application using the token or the purpose of the token.
- Expiration date**
A date picker input field showing 'YYYY-MM-DD'.
- Select scopes**
Scopes set the permission levels granted to the token. [Learn more.](#)
- 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).
- Create personal access token** (button)

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

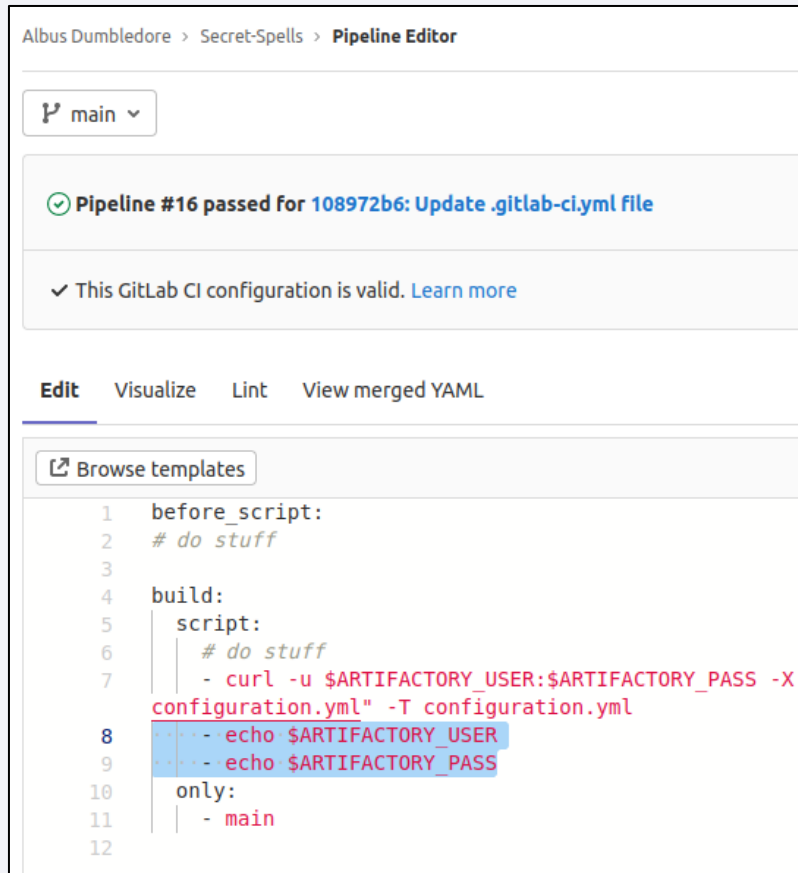
- 'post' AND 'personal_access_tokens'
- 'post' AND 'profile/keys'
- 'post' AND 'personal_access_tokens'
- 'post' AND 'user/keys'

```
r:~# cat /var/log/gitlab/gitlab-rails/production.log | grep -A3 -i post
profile/personal_access_tokens" for 192.168.1.54 at 2022-01-27 14:03:2
files::PersonalAccessTokensController#create as HTML
authenticity_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
se_category":"authentication and authorization","meta_client_id":"user
```

```
api_json.log | grep -i post | grep -i 'user/keys'
uration_s":0.01929,"db_duration_s":0.00046,"view_duration_s":0.01883,"st
S9cVISn08JpJQ8JKSnKNSjodEuKL5y3 4qahM4owbqIcjmM17Kr0AqESn0GGmBB5ks9FECbu
C93 LEqMu0IidE/AgIJP/p3QQR4WRnGvErNbgJIPU1IHeHA7wSxgC/o4btbrkfoyoYkLf3n1
68.1.54, 127.0.0.1","ua":"curl/7.68.0","route":"/api/:version/user/keys'
nt":1,"db_primary_cached_count":0,"db_primary_wal_count":0,"db_primary_v
d":"01FTEHE2Z6GTKM2570GBC086V1","meta.caller_id":"POST /api/:version/use
```

Modifying CI/CD Pipeline

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



The screenshot displays the GitLab Pipeline Editor interface for the project 'Albus Dumbledore > Secret-Spells'. The current branch is 'main'. A notification indicates that 'Pipeline #16 passed for 108972b6: Update .gitlab-ci.yml file'. Below this, a message states 'This GitLab CI configuration is valid. Learn more'. The interface includes tabs for 'Edit', 'Visualize', 'Lint', and 'View merged YAML'. A 'Browse templates' button is also visible. The main area shows the content of the `.gitlab-ci.yml` file:

```
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
```


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 Database -

```
gitlabhq_production=> select id,username,encrypted_password,admin,state,otp_required_for_login,otp_backup
id | username | encrypted_password | admin | state | otp_r
-----+-----+-----+-----+-----+-----
 3 | rweasley | $2a$10$7zCL9VNMzUwNgnA7BIsT4u68A8enr0FEM4pxvYESooCicgrQkRD/0 | f | active | f
 1 | root | $2a$10$Xnk4uLy4oy3YE66EkJqzreUqCav/udoNyhv6xLC6QzxK8TrdW0QaG | t | active | f
 6 | ssnape | $2a$10$8ZSV08sItD.lQ1uiUGJJyuWpOKzeXhdm08LDf8JE20mX5tQ9DnA5e | f | active | f
 2 | hpotter | $2a$10$SHrY1lsI3u6v/sYBbBRhtc.Zq81LcNg/8cEmcrDgf/LNT4D/fFNtsa | f | active | f
 5 | adumbledore | $2a$10$BdEKz1CBfC2BTjYfPj1HPuDt.gU08PF6cPNn0fuL00iusfLGt02Ge | 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

Branch Permissions

- Prevent all changes, Prevent deletion, Prevent rewriting history, Prevent changes without a pull request

Access Token Scopes

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

API Capabilities

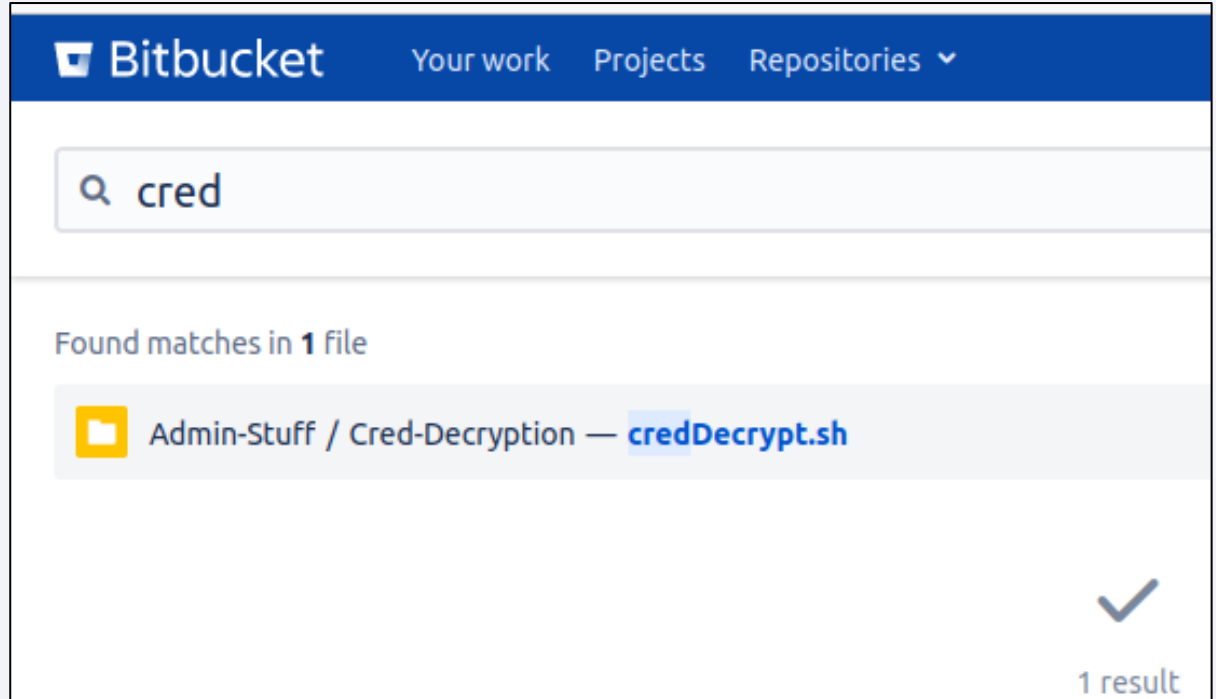
- REST API
- Interact with:
 - Repositories
 - SSH Keys
 - Users
 - Admin functionality
 - And much more...

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

- Interact with 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/atlassian-bitbucket.log | grep -i post | grep -i search | grep -i query
:00,327 DEBUG [http-nio-7990-exec-10] bitbucket-admin @1GXX8USx842x109x1.54 "POST /rest/search/latest/search HTTP/1.1" c.a.b.i.s.s.DefaultSearch 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.DefaultSearch query: {
:00,512 DEBUG [http-nio-7990-exec-10] bitbucket-admin @1GXX8USx842x109x1.54 "POST /rest/search/latest/search HTTP/1.1" c.atlassian.bitbucket.search: 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.search: 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.DefaultSearch query: {
:00,642 DEBUG [http-nio-7990-exec-9] bitbucket-admin @1GXX8USx843x111x2.54 "POST /rest/search/latest/search HTTP/1.1" c.atlassian.bitbucket.search: 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

The screenshot shows the Bitbucket Administration interface. The top navigation bar includes the Bitbucket logo, 'Your work', 'Projects', and 'Repositories'. A search bar is present with the text 'Search for code, commits or repositories...'. The main content area is titled 'Administration' and has a sidebar on the left with various menu items. The 'Global permissions' section is active, showing a table of user access. The table has columns for 'Name', 'System Admin', 'Admin', 'Project Creator', and 'Bitbucket User'. The 'Admin' column for 'Hermoine Granger' is highlighted with a red box, indicating that this user is being promoted to the Admin role.

Name	System Admin	Admin	Project Creator	Bitbucket User
<input type="text" value="Add Users"/>				Bitbucket User
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

Audit Log

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

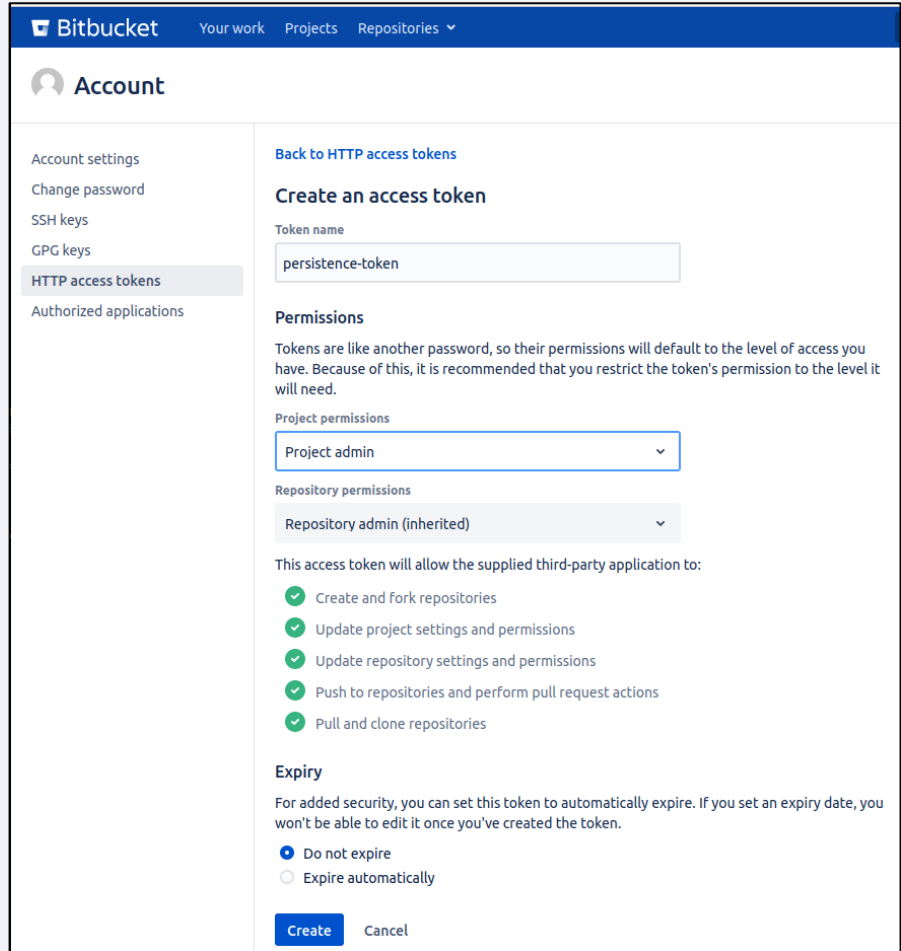
Search Criteria

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

```
lassian/application-data/bitbucket/log/atlassian-bitbucket-access.log | g  
| - | 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 H
```

Maintain Persistent Access

- Personal Access Token
- SSH Key



The screenshot shows the Bitbucket 'Account' settings page. The left sidebar contains navigation options: Account settings, Change password, SSH keys, GPG keys, HTTP access tokens (highlighted), and Authorized applications. The main content area is titled 'Back to HTTP access tokens' and 'Create an access token'. It includes a 'Token name' input field with the value 'persistence-token'. Below this is the 'Permissions' section, which states that tokens are like passwords and should be restricted. It features two dropdown menus: 'Project permissions' set to 'Project admin' and 'Repository permissions' set to 'Repository admin (inherited)'. A summary of permissions is listed with green checkmarks: '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'. The 'Expiry' section has two radio buttons: 'Do not expire' (selected) and 'Expire automatically'. At the 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`

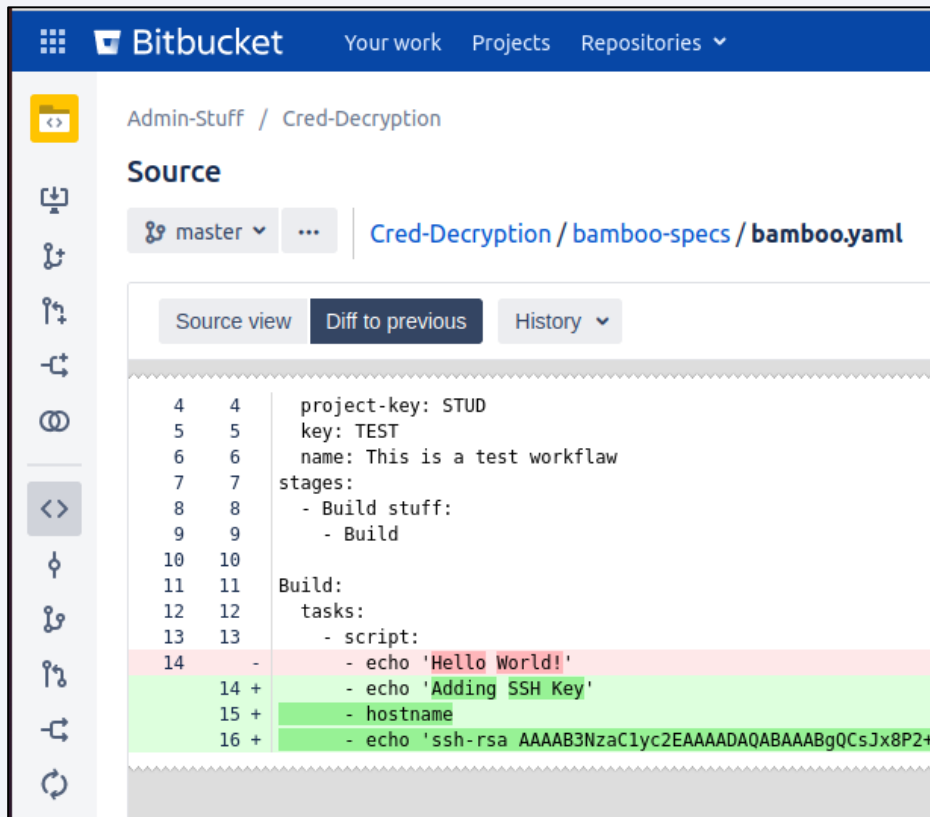
Search Criteria

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

```
bitbucket/log/atlassian-bitbucket-access.log | grep -i post | gre
12 | "POST /rest/analytics/1.0/publish/bulk HTTP/1.1" | "http:/
8:30,517 | "POST /rest/analytics/1.0/publish/bulk HTTP/1.1" | "
15 | "POST /rest/analytics/1.0/publish/bulk HTTP/1.1" | "http:/
9:10,428 | "POST /rest/analytics/1.0/publish/bulk HTTP/1.1" | "
61 | "POST /plugins/servlet/ssh/account/keys/add HTTP/1.1" | "h
9:28,261 | "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 automatically



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/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

external	internal	listener	user	computer
192.168.1.21	192.168.1.21	https	hpotter	DESKTOP-JVKG0R8


```
beacon> inlineExecute-Assembly --dotnetassembly /home/hawk/Toolkit/SCMKit.exe --assemblyargs -s bitbucket
[*] Running inlineExecute-Assembly by (@anthemtothego)
[+] 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

external	internal	listener	user	computer ^
192.168.1.21	192.168.1.21	https	hpotter	DESKTOP-JVKG0R8


```
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	<code>/var/log/github-audit.log*</code>
Management Log	<code>/var/log/enterprise-manage/unicorn.log*</code>
HAProxy Log	<code>/var/log/haproxy.log</code>

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	<code>/var/log/gitlab/gitlab-rails/application.log</code>
	<code>/var/log/gitlab/gitlab-rails/application_json.log</code>
Production Log	<code>/var/log/gitlab/gitlab-rails/production_json.log</code>
	<code>/var/log/gitlab/gitlab-rails/production.log</code>
API Log	<code>/var/log/gitlab/gitlab-rails/api_json.log</code>
Web Log	<code>/var/log/gitlab/nginx/gitlab_access.log</code>

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	'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

Access and Authorization

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

SCM System Configuration Guidance

Repository Access and Code Commits

- Policy of least privilege
- Code branches deleted in a timely manner
- Require at least one approver for each code commit
- Require signed commits via GPG keys or S/MIME certificates

Logging

- Increase logging level to detect reconnaissance 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>

The image features the IBM logo, which consists of the letters 'IBM' in a bold, sans-serif font. Each letter is composed of eight horizontal white stripes of equal thickness and height, set against a dark red-to-black gradient background. The logo is centered horizontally and vertically in the frame.

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>