DEVBRIDGE GROUP

ENGINEERING VALUE

Fuzzing Machine

By Nikolaj Tolkačiov

Agenda

- What is web application fuzz testing
- Introduction to “Fuzzing Machine”
- What results it produces
- Youtube setup in “Fuzzing Machine”
- How it can be used in other projects

What is web application fuzz testing?

Description for fuzzing I

Fuzz testing or **Fuzzing** is a Black Box software testing technique, which basically consists in finding implementation bugs using malformed/semi-malformed data injection in an automated fashion.

Source: OWASP

Description for fuzzing II

Fuzzing or **fuzz testing** is a software testing technique, often automated or semi-automated, that involves providing invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions such as crashes, or failing built-in code assertions or for finding potential memory leaks. Fuzzing is a form of random testing commonly used to test for security problems in software or computer systems.

Source: Wikipedia

Fuzzing types

- Application fuzzing
- File format fuzzing
- Protocol fuzzing
- …

Introduction to “Fuzzing Machine”

Fuzzing Machine

Fuzzing Machine is a dedicated hardware and software setup to perform fuzzing on web applications for extended amount of time and with reporting capabilities.

Core setup consists of:

- Dedicated PC
- Task Scheduler
- SMTP service (SendGrid)
- PowerShell

Concept for fuzzing web application

1. **Launch web browser.**
2. **Navigate to the page where you want to start fuzzing.**
3. **Begin fuzzing.**
4. **Wait.**
5. **Collect logs** (*Optional*)**.**
6. **Rinse and repeat.**

Demo

What results it produces?

Possible artifacts

- Error logs in server side logging.
- Error logs in client side logging.
- Screenshots when error occur.
- Video recording of fuzzing in progress.
- Bug traces to follow in application performance monitoring tools.

Possible artifacts example

```
00:43:42 SEVERE: https://tpc.googlesyndication.com/sadbundle/$csp%3Der3$/13707944800532712673/images/Exp_Big.png - Failed to load resource: the server responded with a status of 404 ()

02:00:41 SEVERE: chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm/cast_sender.js - Failed to load resource: net::ERR_FAILED

02:03:41 SEVERE: https://www.youtube.com/share_ajax?action_get_share_info=1&feature=player_embedded - Failed to load resource: the server responded with a status of 400 ()

04:33:42 SEVERE: https://www.youtube.com/yts/jsbin/player-en_GB-vflzvBT66/base.js 54:13 Uncaught TypeError: Cannot read property 'prototype' of undefined

02:13:42 SEVERE: https://www-opensocial.googleusercontent.com/gadgets/rpc/rpc.v.js 22:16 Uncaught TypeError: Cannot read property 'register' of undefined

09:23:42 SEVERE: https://content.googleapis.com/youtubei/v1/account/accounts_list?alt=json&key=AIzaSyBkrqhJXxYjHdAvok - Failed to load resource: the server responded with a status of 401 ()

07:23:42 SEVERE: https://youtubei.youtube.com/youtubei/v1/log_interaction?alt=json&key=AIzaSyAO_FJ2SlqUTE_Y9_11qcW8 - Failed to load resource: the server responded with a status of 400 ()

12:43:42 SEVERE: https://www.youtube.com/ad_companion?adformat=2_2_1&p=UCXiNIx&render=video_wall_companion&content=jZR-1svUs 74:6 Uncaught ReferenceError: yt is not defined

16:43:42 SEVERE: https://www.youtube.com/yts/jsbin/www-en_US-vflZkT0AY/base.js 715:402 Uncaught TypeError: Cannot read property 'startsWith' of undefined

02:08:41 SEVERE:https://ad.atdmt.com/i/img;adv=11112202503514;ec=11112202508902;adv.a=101108;c.a=817825;s.a=860385;p.a=2577404;as.a=2577404;a.a=17847527;
cache=%7BCACHEBUSTER%7D;https://ad.atdmt.com/i/img;adv=11112202503514;ec=11112202508902;adv.a=101108;c.a=817825;s.a=860385;p.a=2577404;as.a=2577404;a.a=17847527;
cache=%7BCACHEBUSTER%7D;?rnd=45473 - Failed to load resource: the server responded with a status of 404 ()

03:23:41 SEVERE: https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-6219811747049371&output=js&adk=511001906&adf=3383700283& loeid=9422596%2C9%0349%%2C20040077
&num_ads=1&channel=pyvhome%2Bhitchhiker%2Bpyv-top-right-homepage%2Bpyv-top-right-homepage-us%2Bytdevice_1%2B4311047448%2Bpyvhome_LT%2Blogged-
out%2Bpyvhomeinshelf&ad_type=text&ea=0&flash=24.0.0&hl=en&url=https%3A%2F%2Fwww.youtube.com%2Fchannel%2FUCOpNcN46UbXVtpKMrmU4Abg&wgl=1&pyv=1&dt=1489195243538&b
dt=2941&idt=198&shv=r20170308&cbv=r20170110&saldr=sb&correlator=8312176288284&frm=23&ga_vid=911827537.1489195244&ga_sid=1489195244&ga_hid=1023032743&ga_fc=0&pv=2&iag=3&
icsg=10&nhd=1&dssz=4&mdo=0&mso=0&u_tz=120&u_his=3&u_java=0&u_h=900&u_w=1600&u_ah=860&u_aw=1600&u_cd=24&u_nplug=5&u_nmime=7&biw=1583&bih=794&isw=300&ish=110&ifk
=919813956&eid=40509013&oid=3&loc=EMPTY&top=https%3A%2F%2Fwww.youtube.com%2Fchannel%2FUCOpNcN46UbXVtpKMrmU4Abg&rx=0&eae=2&fc=16&brdim=0%2C0%2C0%2C0%2C160
0%2C0%2C1600%2C860%2C300%2C110&vis=1&rsz=o%7Co%7Cpr%7C&abl=NS&ppjl=u&fu=4180&bc=1&ifi=1&dtd=259 - Failed to load resource: the server responded with a status of 400 ()
```

Bugs likely to find with fuzz testing

- Null pointer exceptions
- Application crashes
- Unexpected combinations as input
- Server and client side validation issues

Youtube setup in “Fuzzing Machine”

Recipe for fuzzing

1 **webdriver-manager**

1 **protractor**

1 **Gremlins.js**

9 lines of JavaScript for fuzzing commands

1 cup of code for **navigating and logging errors to file**

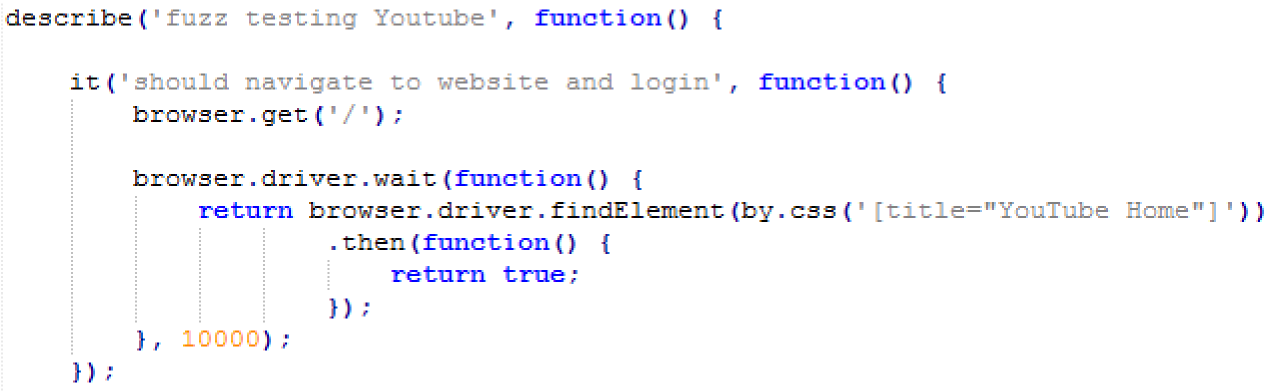
3 **scheduled jobs** to keep it running 24/7

11 lines of Command Prompt lines to archive logs

14 lines of power shell scripts to **send email with attachment**

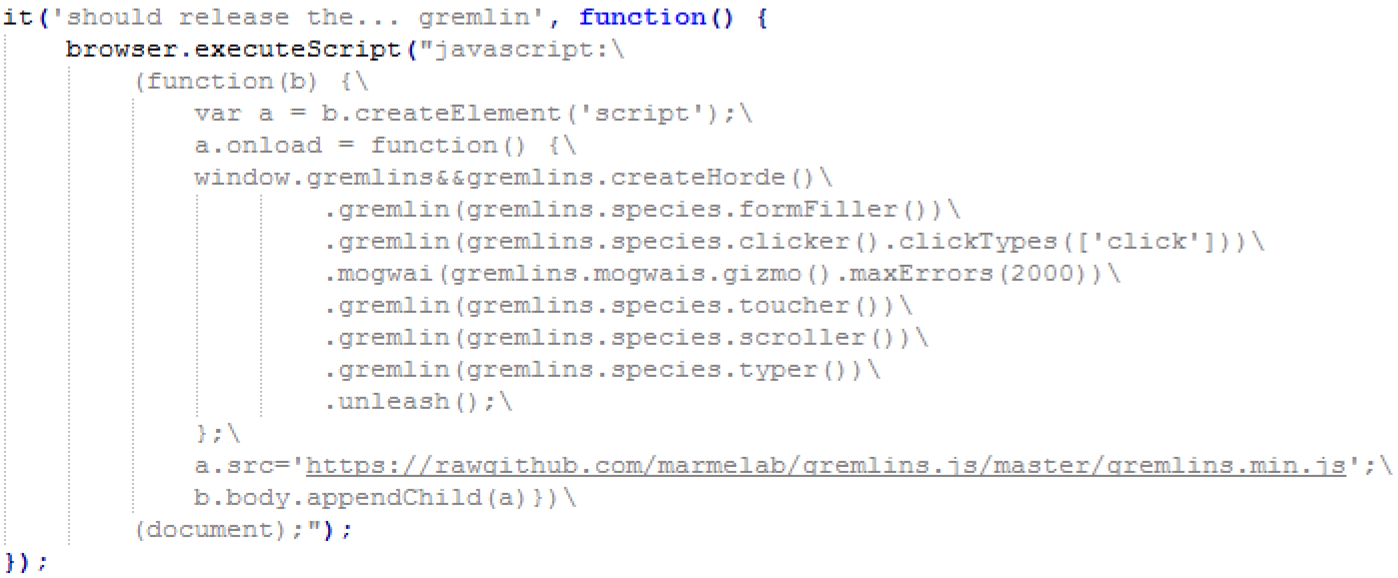
1 **SendGrid** account for email sending purpose

Step 1



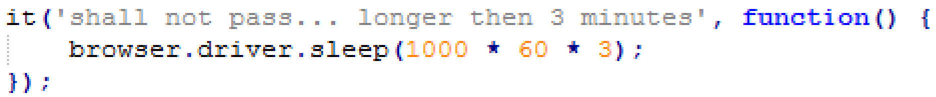
```
describe('fuzz testing Youtube', function() {

    it('should navigate to website and login', function() {
        browser.get('/');

        browser.driver.wait(function() {
            return browser.driver.findElement(by.css('[title="YouTube Home"]'))
                    .then(function() {
                        return true;
                    });
        }, 10000);
    });
```

Step 2



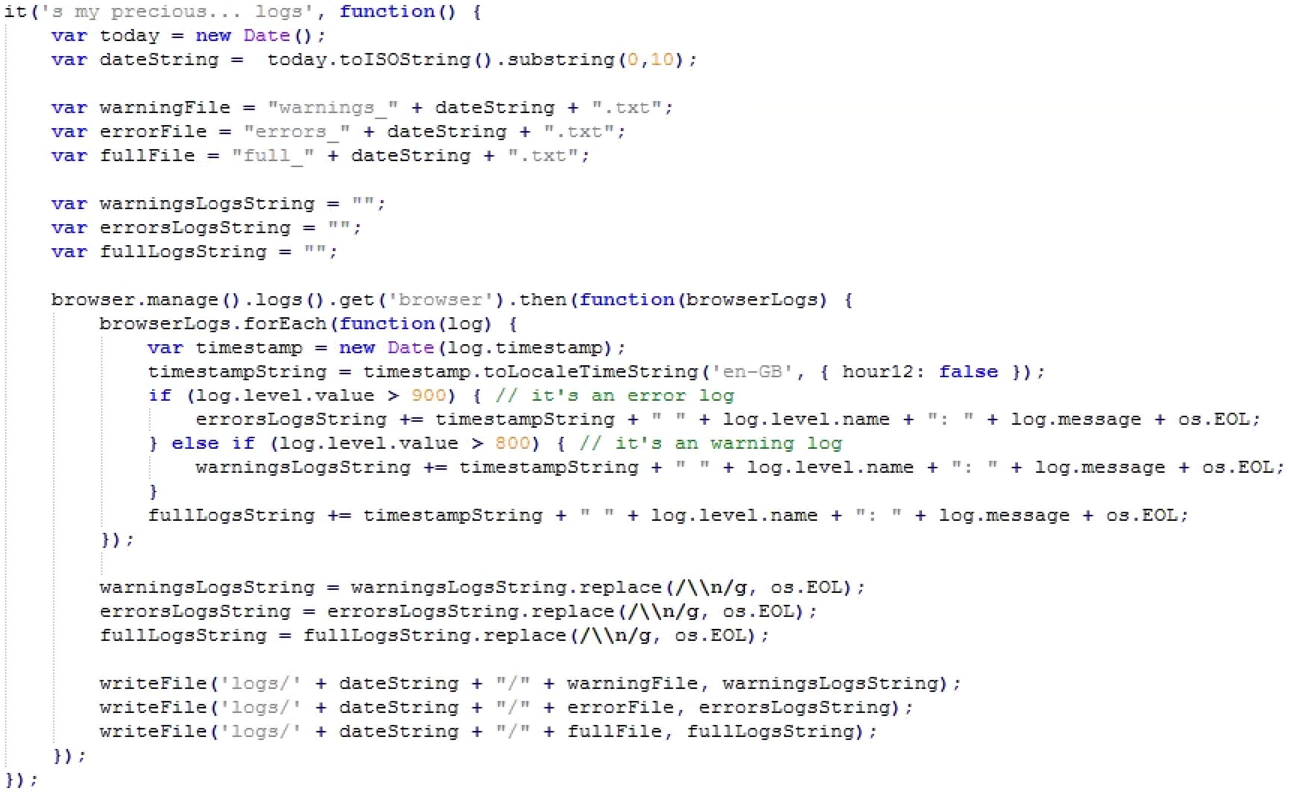
```
it('should release the... gremlin', function() {
    browser.executeScript("javascript:\
        (function(b) {\
            var a = b.createElement('script');\
            a.onload = function() {\
            window.gremlins&&gremlins.createHorde()\
                    .gremlin(gremlins.species.formFiller())\
                    .gremlin(gremlins.species.clicker().clickTypes(['click']))\
                    .mogwai(gremlins.mogwais.gizmo().maxErrors(2000))\
                    .gremlin(gremlins.species.toucher())\
                    .gremlin(gremlins.species.scroller())\
                    .gremlin(gremlins.species.typer())\
                    .unleash();\
            };\
            a.src='https://rawgithub.com/marmelab/gremlins.js/master/gremlins.min.js';\
            b.body.appendChild(a)})\
        (document);");
});
```

Step 3



```
it('shall not pass... longer then 3 minutes', function() {
    browser.driver.sleep(1000 * 60 * 3);
});
```

Step 4

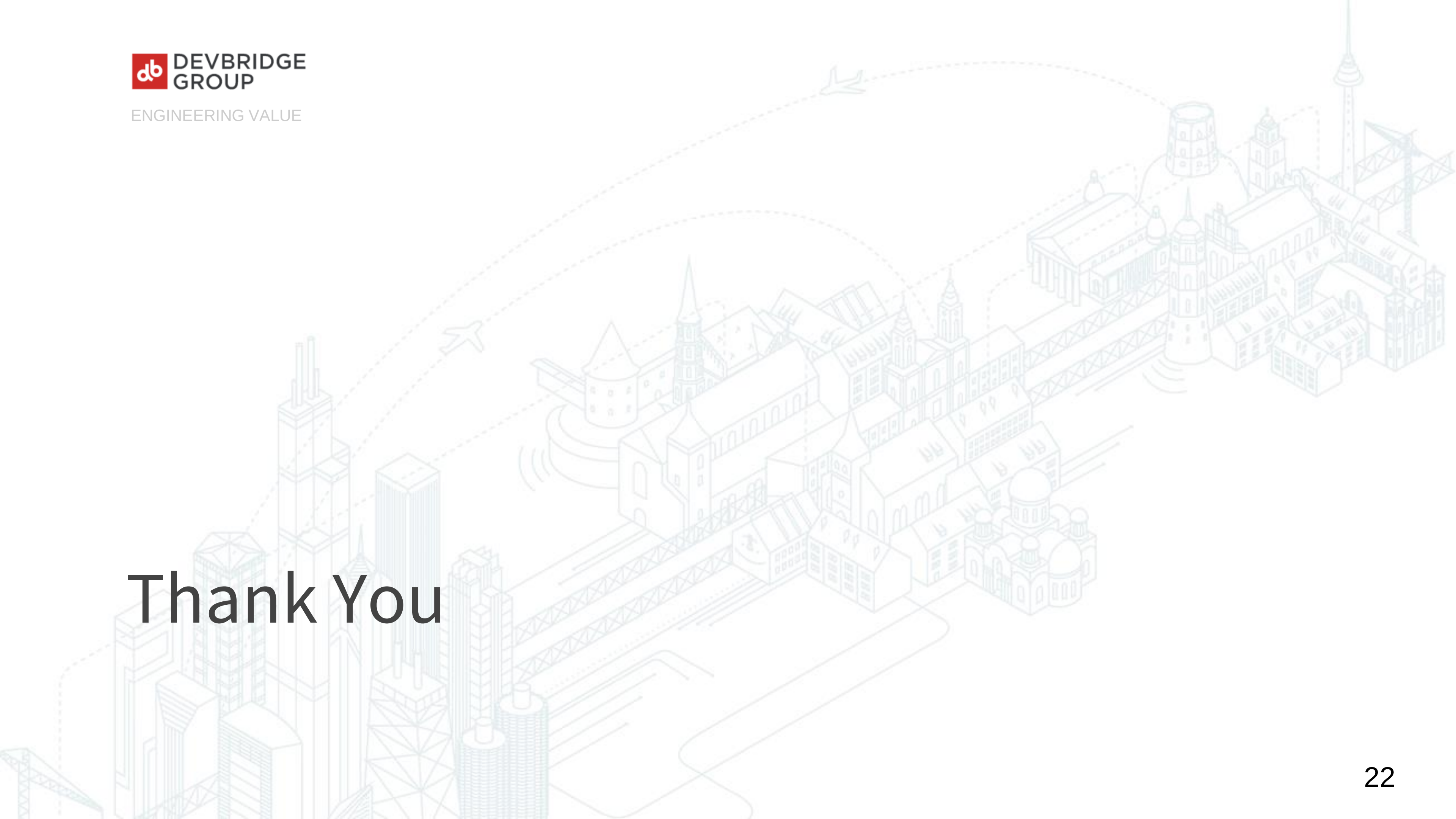


```
it('s my precious... logs', function() {
    var today = new Date();
    var dateString =  today.toISOString().substring(0,10);

    var warningFile = "warnings_" + dateString + ".txt";
    var errorFile = "errors_" + dateString + ".txt";
    var fullFile = "full_" + dateString + ".txt";

    var warningsLogsString = "";
    var errorsLogsString = "";
    var fullLogsString = "";

    browser.manage().logs().get('browser').then(function(browserLogs) {
        browserLogs.forEach(function(log) {
            var timestamp = new Date(log.timestamp);
            timestampString = timestamp.toLocaleTimeString('en-GB', { hour12: false });
            if (log.level.value > 900) { // it's an error log
                errorsLogsString += timestampString + " " + log.level.name + ": " + log.message + os.EOL;
            } else if (log.level.value > 800) { // it's an warning log
                warningsLogsString += timestampString + " " + log.level.name + ": " + log.message + os.EOL;
            }
            fullLogsString += timestampString + " " + log.level.name + ": " + log.message + os.EOL;
        });

        warningsLogsString = warningsLogsString.replace(/\\n/g, os.EOL);
        errorsLogsString = errorsLogsString.replace(/\\n/g, os.EOL);
        fullLogsString = fullLogsString.replace(/\\n/g, os.EOL);

        writeFile('logs/' + dateString + "/" + warningFile, warningsLogsString);
        writeFile('logs/' + dateString + "/" + errorFile, errorsLogsString);
        writeFile('logs/' + dateString + "/" + fullFile, fullLogsString);
    });
});
```

How it can be used in other projects?

DEVBRIDGE GROUP

ENGINEERING VALUE



Thank You