Scientific and Practical Cyber Security Journal (SPCSJ) 2(2):25-27
Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667

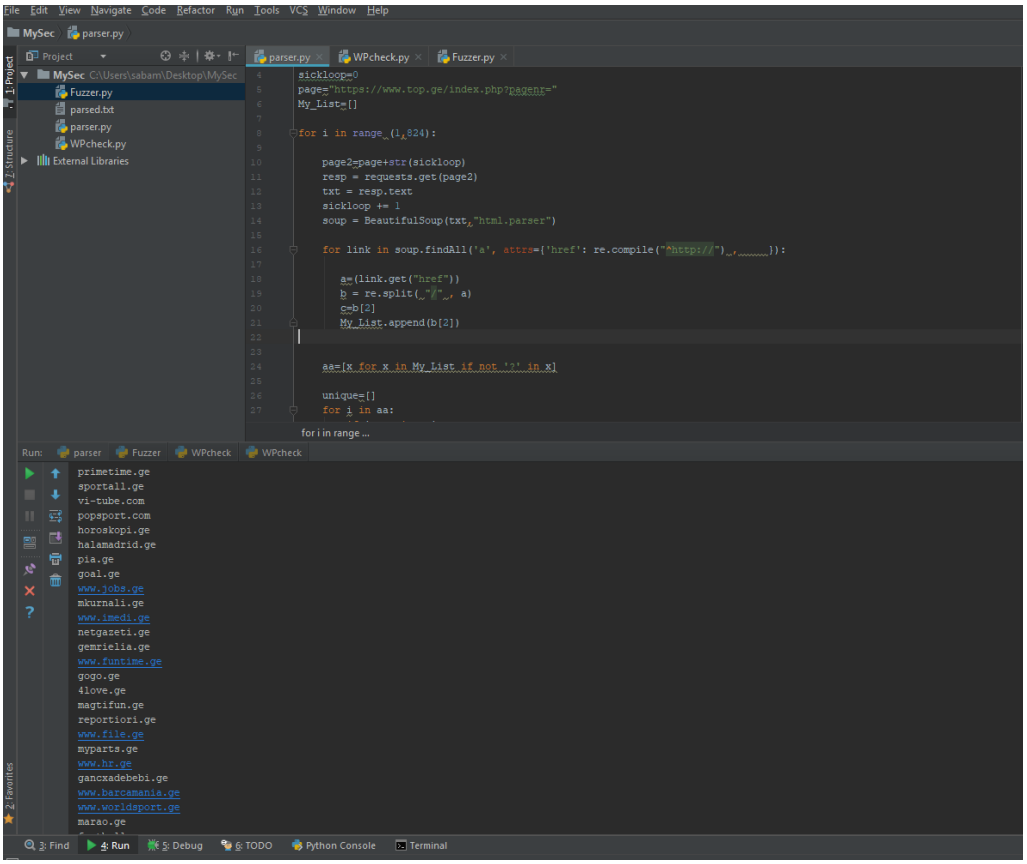
ATTACKS ON WEBSITES WITH INAPPROPRIATE STRUCTURE

Saba Meskhi
Business and Technology University, Tbilisi, Georgia

ABSTRACT

The article concerns the problems of Georgian web developers and cyber security issues related with these problems, that are demonstrated and revealed using testing methods.

როგორ შეიძლება, გულუბრყვილობამ საფრთხე შეუქმნას თქვენს ვებ-საიტს?
განვიხილოთ შემთხვევა როდესაც ადამიანი ტოვებს სახლის გასაღებს აშკარა ადგილას. ქურდს არ აქვს წინასწარი ცოდნა იმის შესახებ, თუ სადაა დამალული გასაღები, მაგრამ შეიძლება ითქვას, რომ თუ ის სავარაუდო და მარტივად პროგნოზირებად ადგილებში დაიწყებდა ძიებას, აუცილებლად მიაგნებდა დაუდევრად გადამალულ სახლის გასაღებს!
კიბერ სივრცეში საიტის ბექაპი აუცილებელია. ასევე აუცილებელია მისი დაცვა [1,2].
დავუშვათ, რომ ჩვენი საიტის ყველა ფაილი ჩვენ მიერ ერთ ფაილში დაარქივდა და დაერქვა, a.zip. ეს ნიშნავს, რომ თუ ვინმე შევა საიტზე - "http://example.com/a.zip" ბრაუზერი ავტომატურად დაიწყებს ამ ფაილის გადმოწერას და კიბერ დამნაშავე ხელში ჩაიგდებს ჩვენი საიტის ბექაპს.
გადავიდეთ პრაქტიკულ ნაწილზე და გავიგოთ, რამდენად მიამიტნი არიან ქართველი დეველოპერები კიბერ ჰიგიენაში.
ამისათვის დავიხმაროთ Top.ge - საიტი, სადაც განთავსებულია ქართული ვებ-გვერდების რეიტინგი.
საიტების დასახელების წამოსაღებად და ტექსტურ ფაილში ჩასაწერად დაიწერა პითონის სკრიპტი.

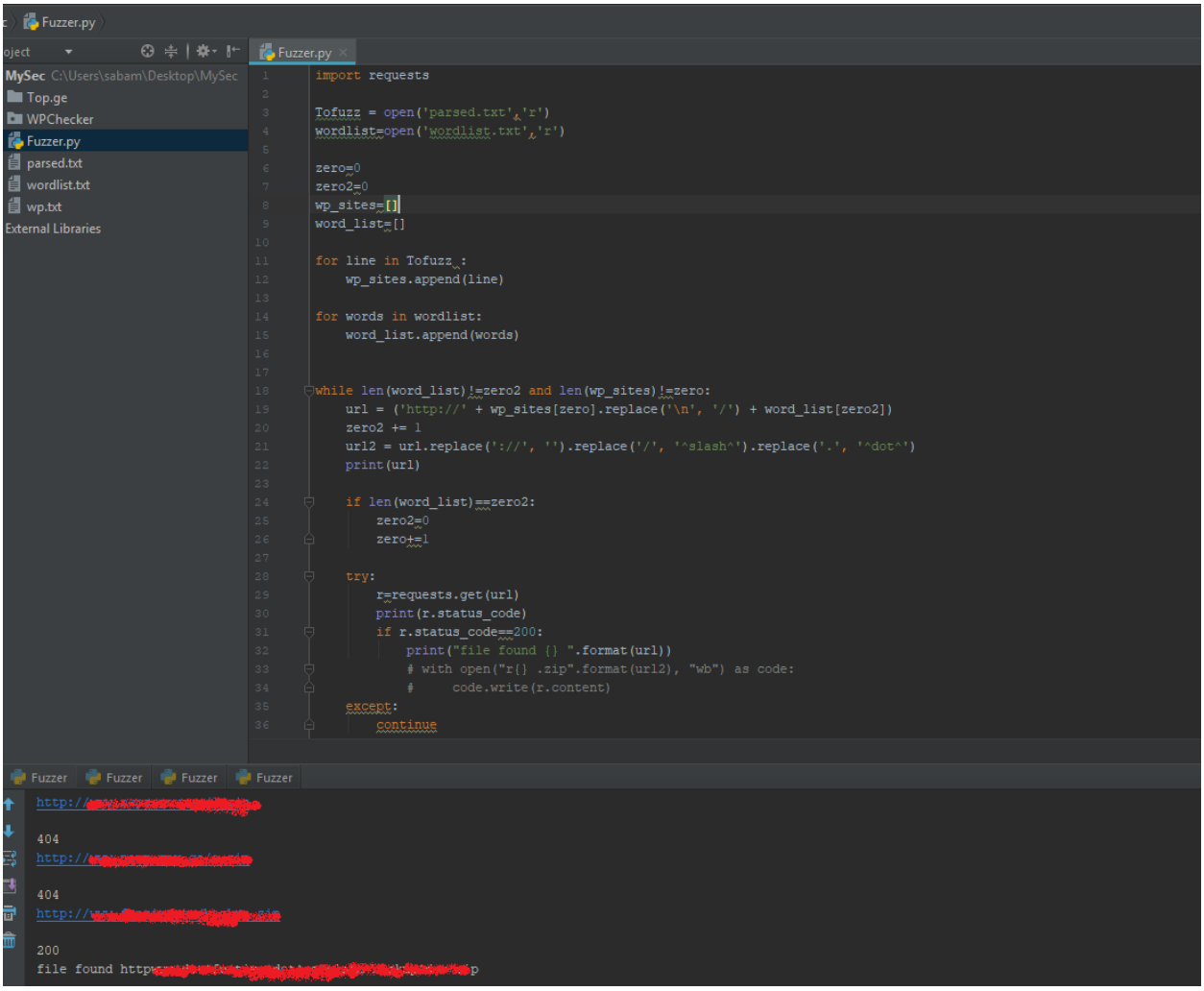


სურათი 1.

სულ გამოვიდა 16000-მდე საიტის დასახელება.
როგორც ქურდმა, ასევე კიბერ დამნაშავემაც არ იცის, სად იმალება საიტის გასაღები , ანუ რა სახელი აქვს საიტის ბექაპს. ამისთვის საჭიროა, ის მოიებნოს მარტივად პროგნოზირებად ადგილებში.
სადემონსტრაციოდ გამოყენებული იყო 4 სავარაუდო დასახელება.

- backup.zip
- backup_old.zip
- 1.zip
- a.zip

დაიწერა სკრიპტი, რომელიც ტექსტური ფიალიდან იღებდა საიტების დასახელებას, და აწყვილებდა სავარაუდო დასახელებებს, ფაილის არსებობის შემთხვევაში კი აბრუნდებდა “200” კოდს.
სკრიპტის გაშვებიდან რამდენიმე წუთში ფაილი, ანუ საიტის გასაღები ნაპოვნია!



სურათი 2.

ამგვარი შემთხვევების თავიდან ასაცილებლად, უნდა შემოწმდეს საიტის დირექციები, ფაილები და მასზე მინიჭებული უფლებები.

REFERENCES

1. Frank McCown , Catherine C. Marshall , Michael L. Nelson, Why web sites are lost (and how they're sometimes found), Communications of the ACM, v.52 n.11, November 2009
2. Frank McCown , Michael L. Nelson, Recovering a website's server components from the web infrastructure, Proceedings of the 8th ACM/IEEE-CS joint conference on Digital libraries, June 16-20, 2008, Pittsburgh PA, PA, USA