NEW
VULN
SEP 2018

LÒKÍDИ

Lapse **o**f **K**eyboard at **I**nternationalized **D**omain **N**ame

LOKIDN is a new kind of vulnerability that
has not been discovered before

Özkan Mustafa AKKUŞ

/siberguvenlik /ehakkus /9483

Lapse of Keyboard at Internationalized Domain Name (LOKIDN)

1.0. Introduction

With the rapidly developing and popularized world wide web, interest in private domain names has also increased considerably. Today, if we consider both corporate/organization and individual based, it is very important to get a domain name suitable for branding and attention purposes.

The increasing need for domain name in the world has given birth to the lack of domain name. It has become almost impossible to rent the desired domain name with the popular TLD (top level domain) extensions(.com .net .org). This has led to the emergence of a new world-wide idea. The countries have been given the opportunity to rent domain names in their native languages and alphabets. In this way, the problem of lack in possible domain names has been desired to be solved. This technology along with phishing attacks also brought the "Lapse of Keyboard at Internationalized Domain Name (LOKIDN)" vulnerability too. This type of vulnerability was officially discovered for the first time by me.

2.0. IDN Structure

As domain names, special characters can be used that are not part of the ASCII character set, thanks to IDN architecture. Normally, domain names are restricted to ASCII character set which comprise characters "a-z, A-Z, 0-9 and '-'". So, how does a domain name based on IDN architecture hence with UNICODE is interpreted to meet regular architecture and vice verse? The UNICODE characters are converted to their corresponding ASCII character format to ensure communication with the server.
For instance; the domain name "lokıdn.com" is interpreted by IDN is "xn--lokdn-p4a.com". That is, when you buy domain name "lokıdn.com", you actually register for "xn--lokdn-p4a.com".

IDN specification is accepted by many countries now and actively being used by them.

3.0. Summary

Complex web applications developers can make technical mistakes in the application development or update phases. Indeed, many of the security vulnerabilities are created by developers or managers. Developers can perform keyboard typing mistakes while showing reference in the app. IDN domains possess security vulnerability in the direction of these reference errors.

LOKIDN vulnerability can occur in country-specific keyboards that use standard Latin alphabet characters that overlap with standard field name (ASCII) characters. Due to the alphabet set of the developer or administrator keyboard, the field name may be incorrectly referenced. This is similar to the fact that security precautions for database inquiries are not taken into web applications due to a small amount of hesitation which cause injection vulnerabilities. Therefore, the attacker can intervene into the system by exploiting this types of security vulnerabilities left by developer or administrator.

LOKIDN vulnerability occurs when system administrator types "lokıdn.com" instead of "lokidn.-com" domain name. By exploiting this vulnerability, the attacker can hire the "lokıdn.com" domain name or “xn--lokdn-p4a.com”, which has never been leased and suitable for renting, to intervene in the sections where the system administrator made a mistake. The vulnerability can also occur with inverse logic.

4.0. How is it exploited?

Lack of Keyboard at Internationalized Domain Name (LOKIDN) vulnerability can be discovered in many different areas. Exploitation procedures can be carried out in the area where the vulnerability exists.

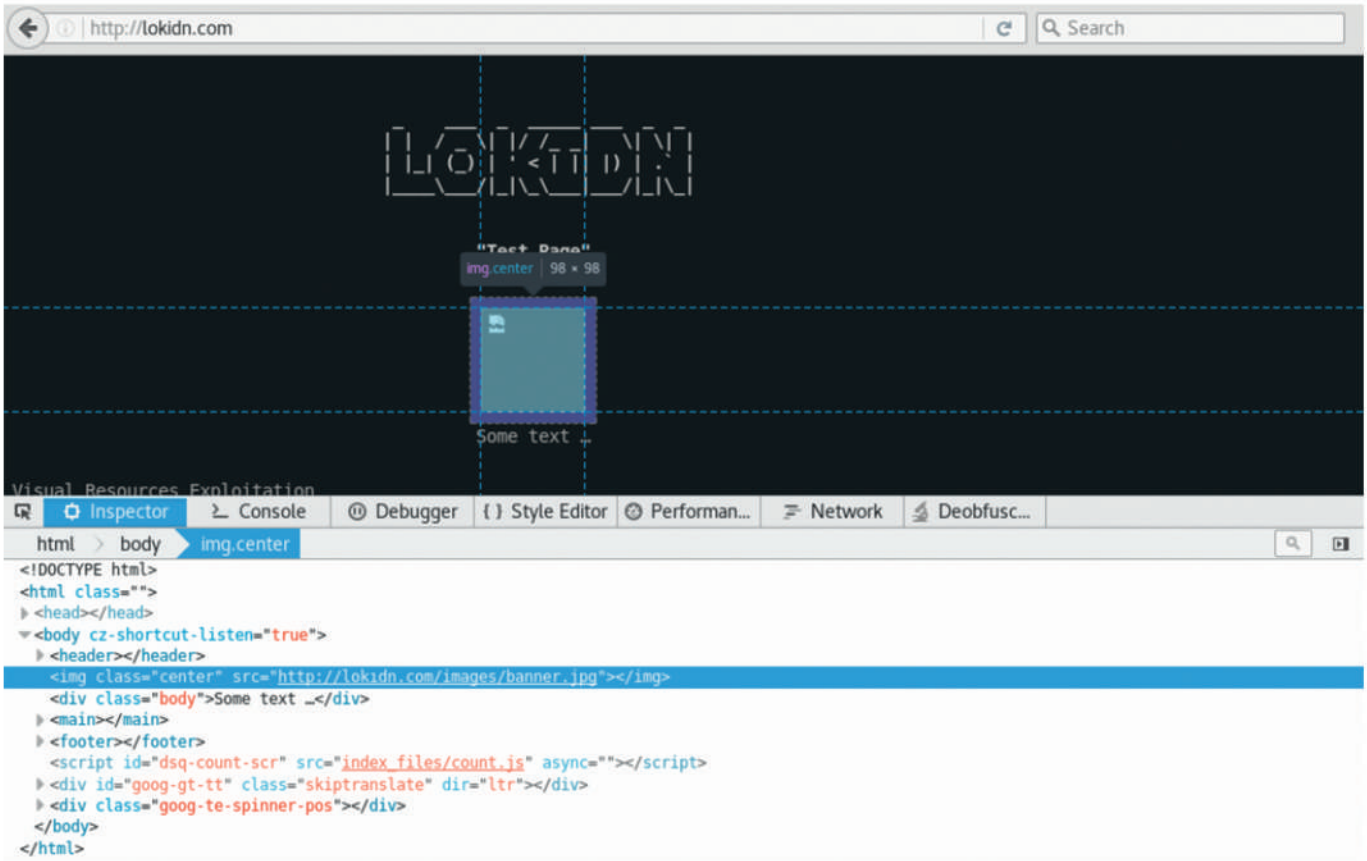
We will examine what exploitation can be done with the general headings.

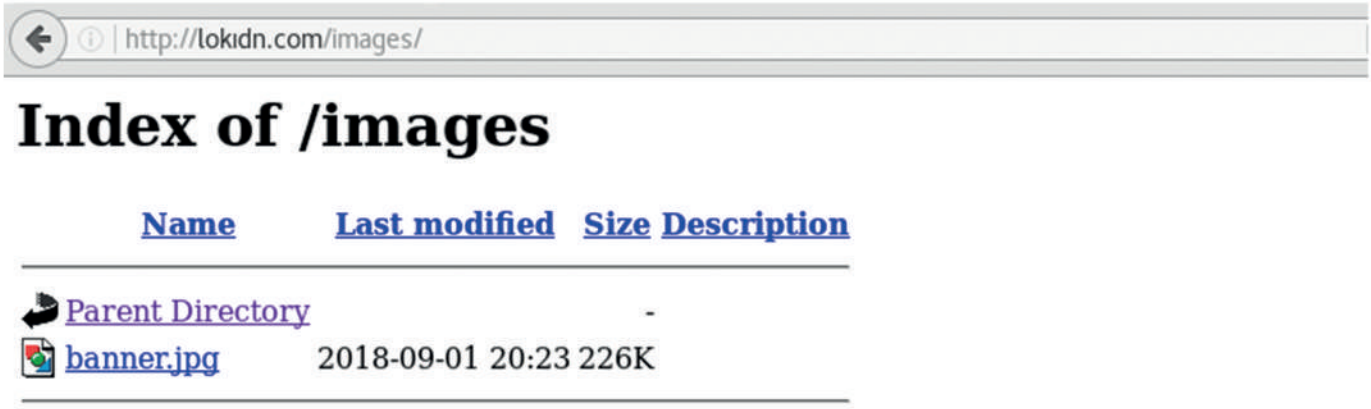
4.1. Visual Resources Exploitation

We see a link that is manually placed on the target site. This source code belongs to the site "lokidn.com". It seems that LOKIDN is weak because of keyboard failure.

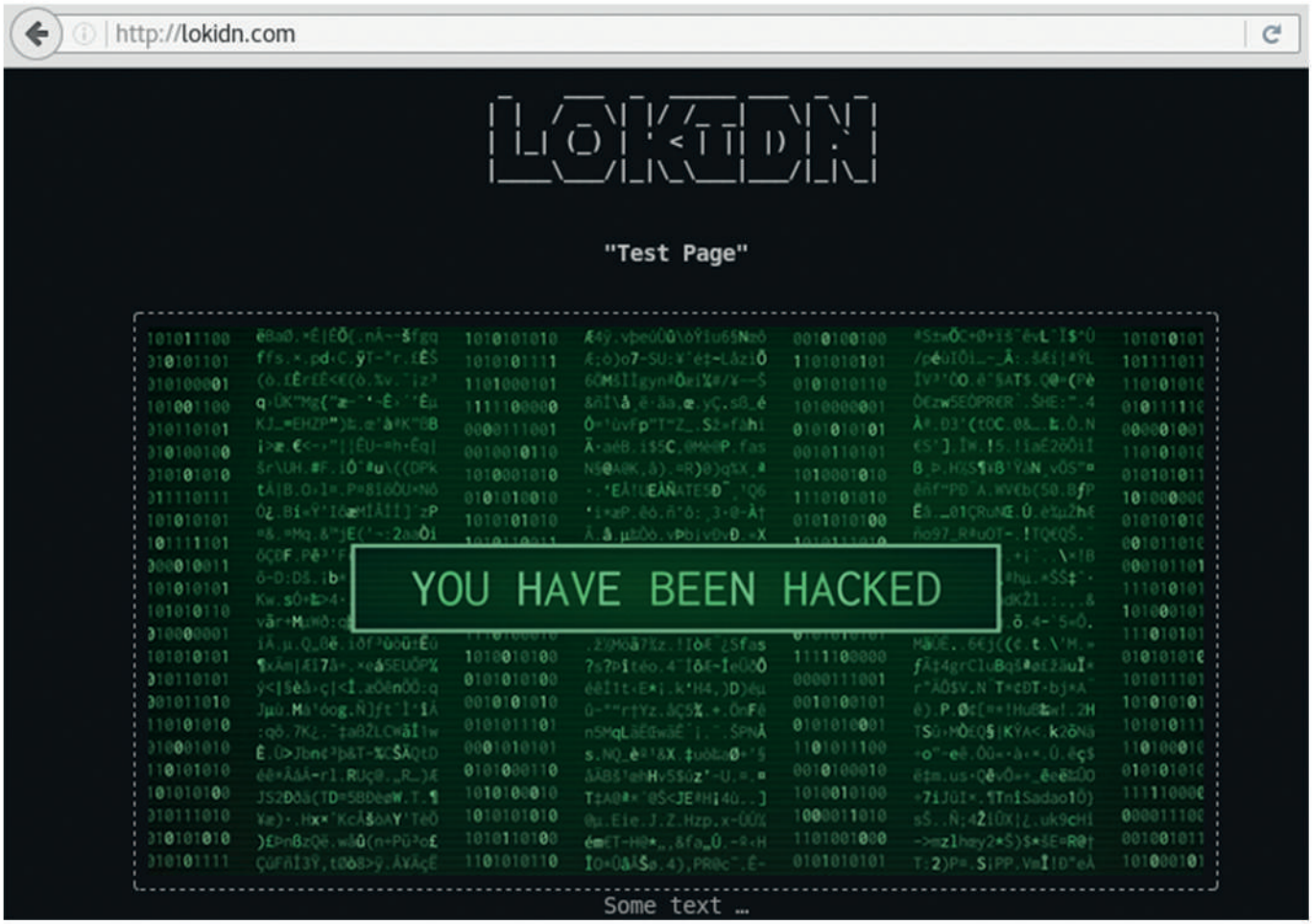
<img class="center" src="http://lokıdn.com/images/banner.jpg"></img>

Therefore, by purchasing the domain name "lokıdn.com", we can intervene in the image located in /images/banner.jpg and place a new visual.





When we renew the address "lokidn.com", we see an image saying that the site is hacked.

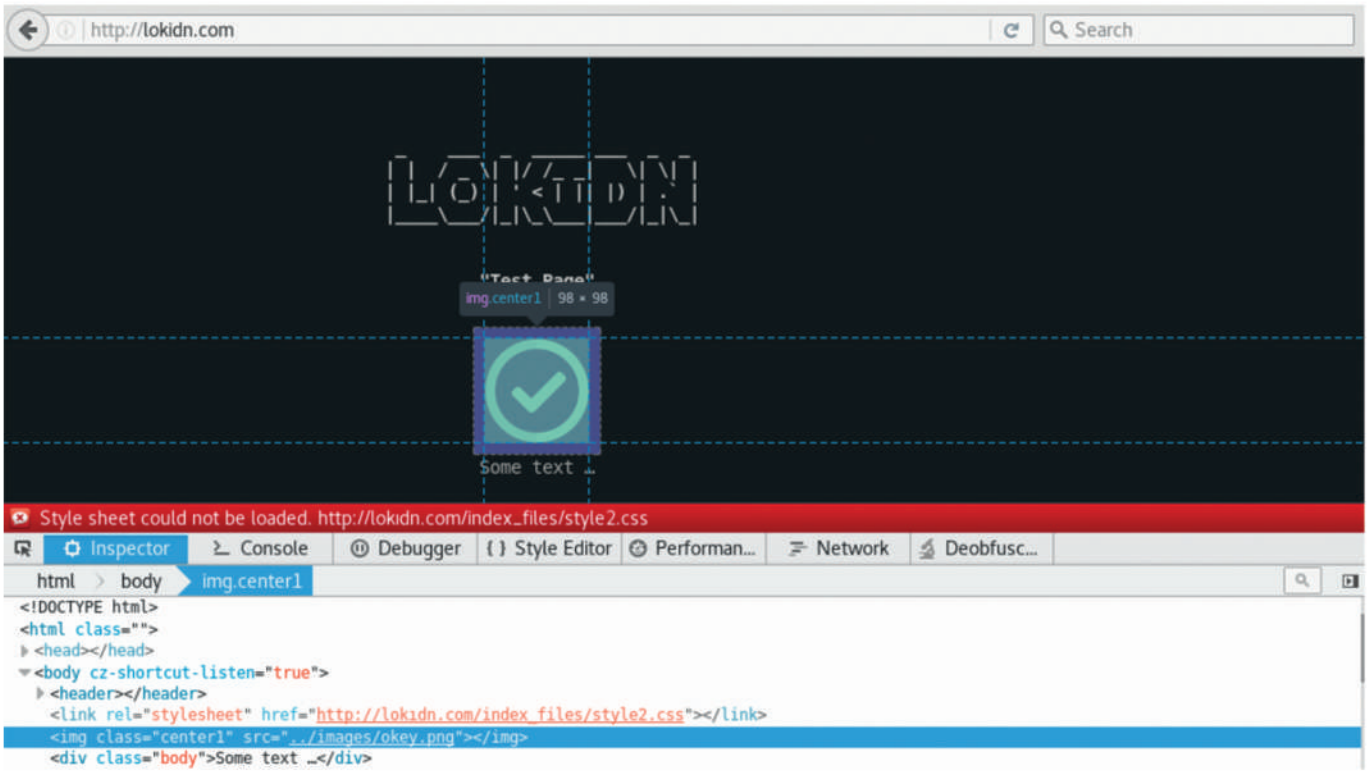


The attacker can do similar actions with LOKIDN vulnerabilities left on the site logos, background, gallery, or visual sources in the ad space.

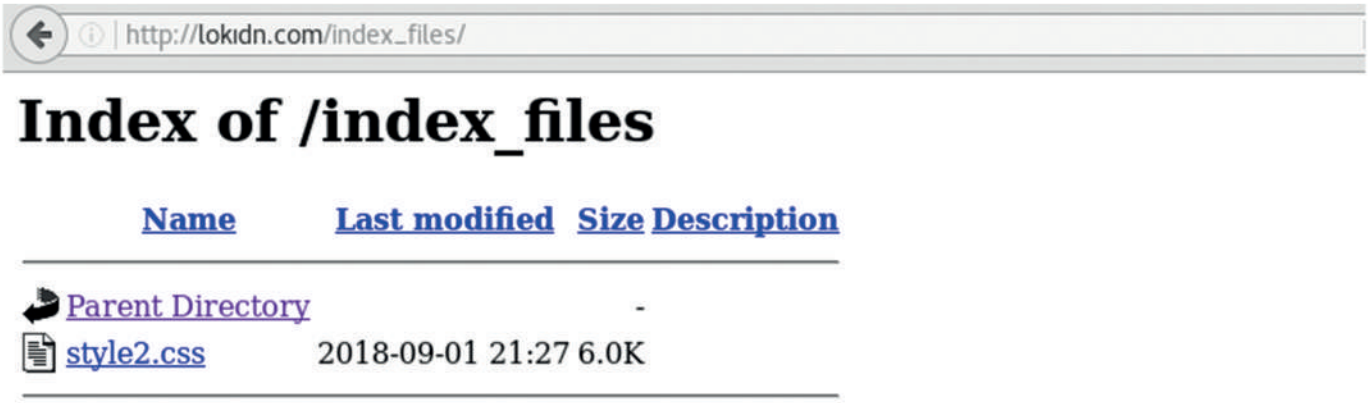
4.2. Style (CSS) Resources Exploitation

An attacker can disrupt or change the appearance of the site with a LOKIDN vulnerability that will be explored in CSS resources, which are indispensable for websites.

In our example, class "center1" does not react correctly due to CSS loss.



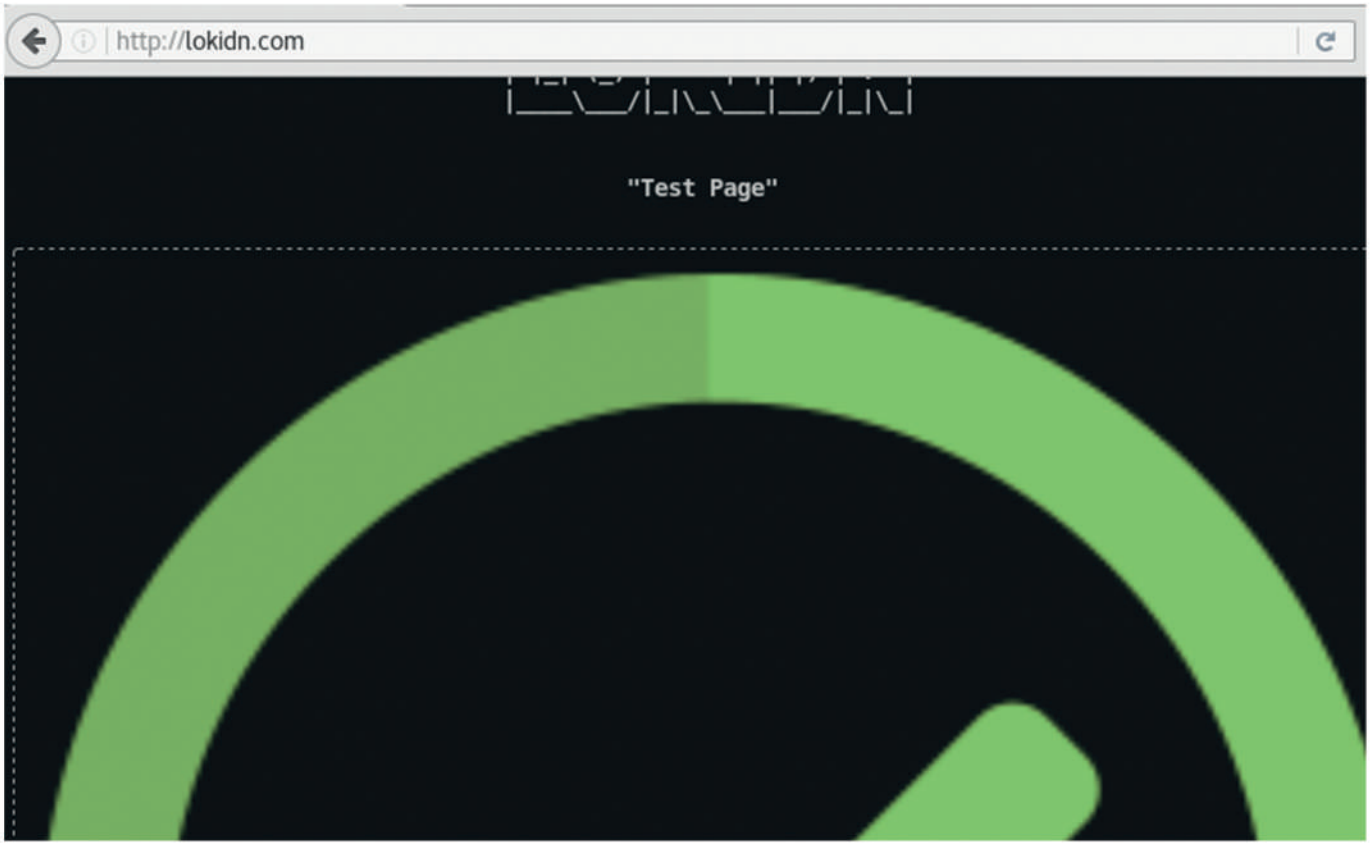
The website is vulnerable to LOKIDN and with that the path of file is exploited.



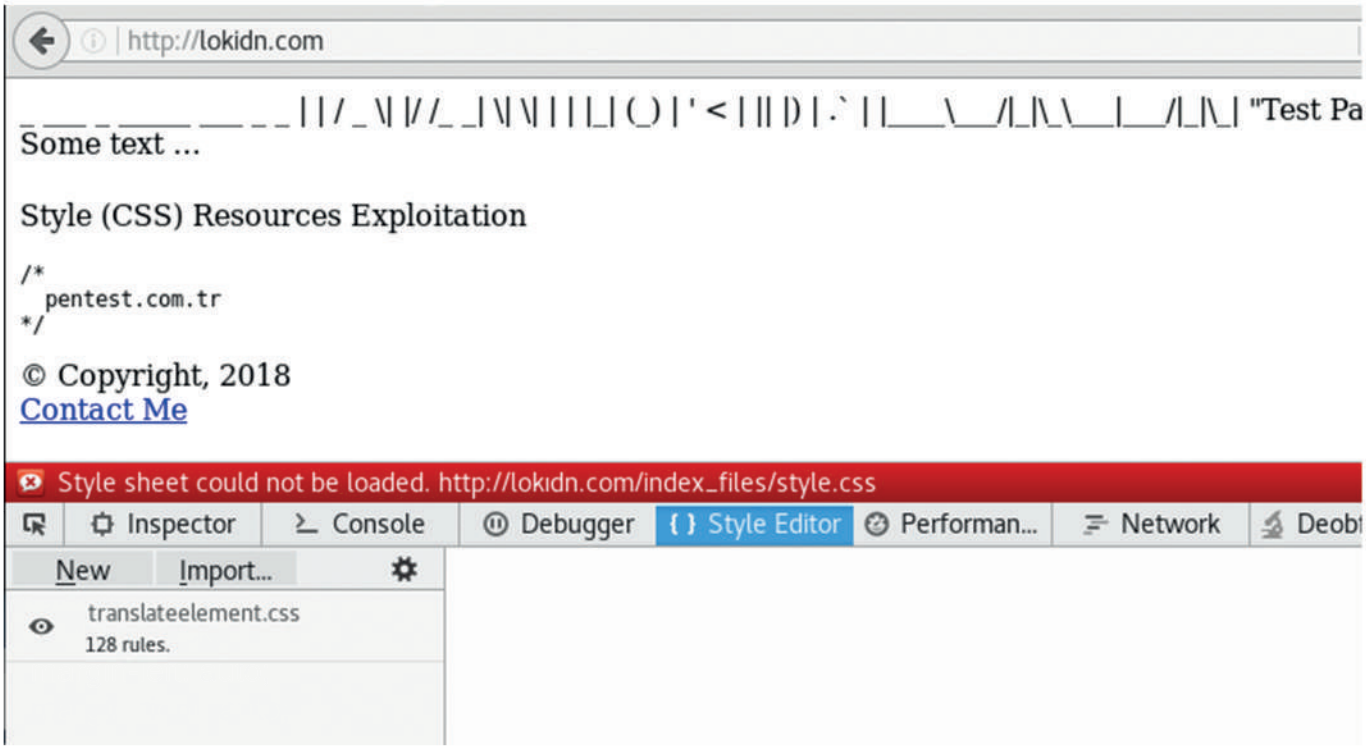
You can now change the visual size of the style2.css file by creating a class called "center 1", which we already know the name.

```
img.center1 {
  display: block;
   margin-left: auto;
   margin-right: auto;
   width: 200%;
   height: 200%;
}
```

By increasing the sizes up to 200% and covering the whole site of the visual, the site can be distorted.



The site's underlying CSS file may also be lost due to the LOKIDN vulnerability. An attacker can play by changing the style of all areas of the site in the same way.

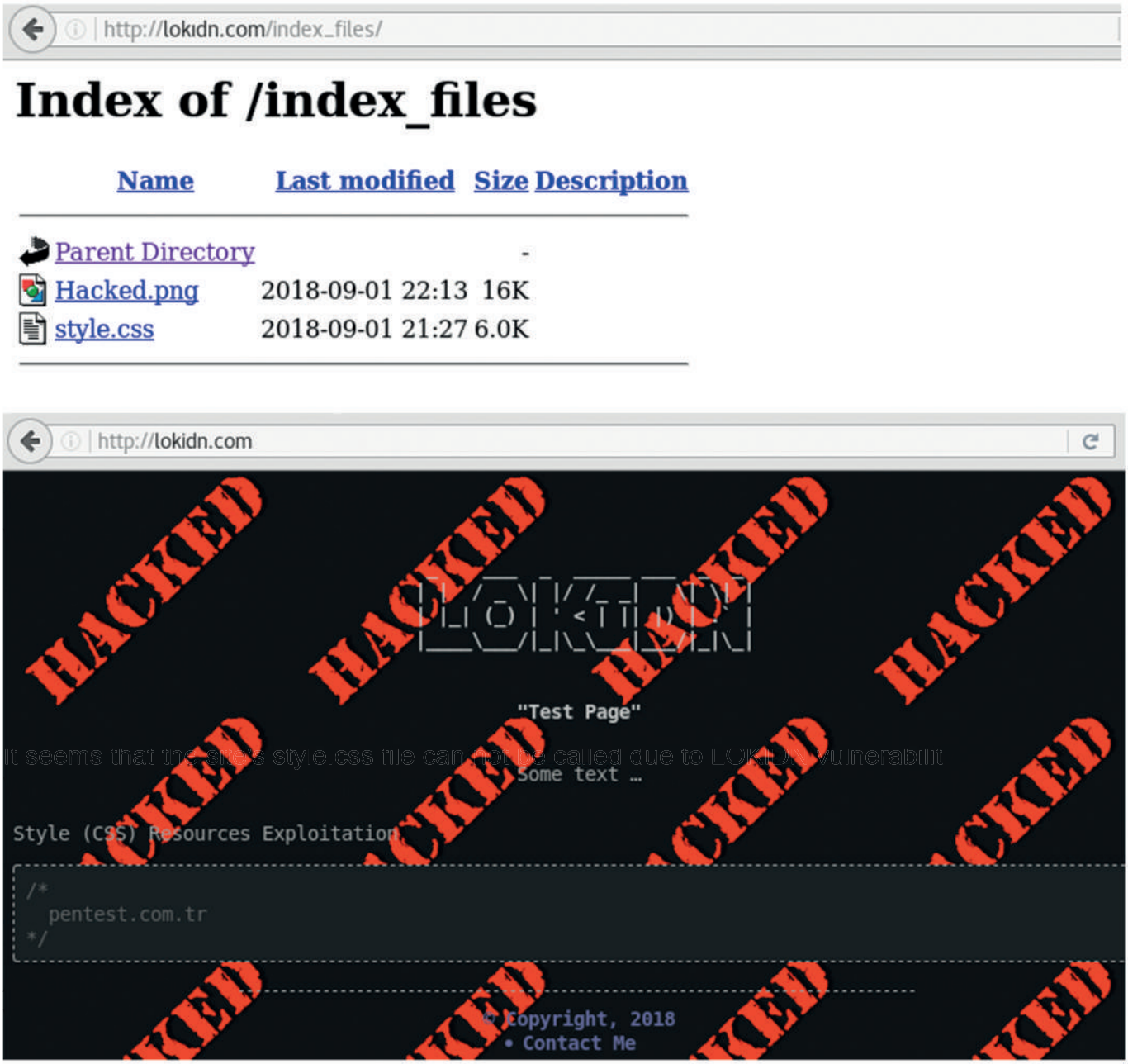


It seems that the site's style.css file can not be called due to LOKIDN vulnerability.
When the source code is examined, it is determined that the "menu" and "body" generic class names are used.

In this direction, a class such as the following can be placed in the content of the file "lokıdn.-com/index_files/style.css".

```
body {
  background-color: #171b1b;
  background-image: url(../index_files/Hacked.png);
}
```

At this point, the attacker can place the desired image in the background of the site.



As shown in the examples, the attacker can modify the CSS file to shape the site with LOKIDN vulnerability.

4.3. Routing to Harmful Target

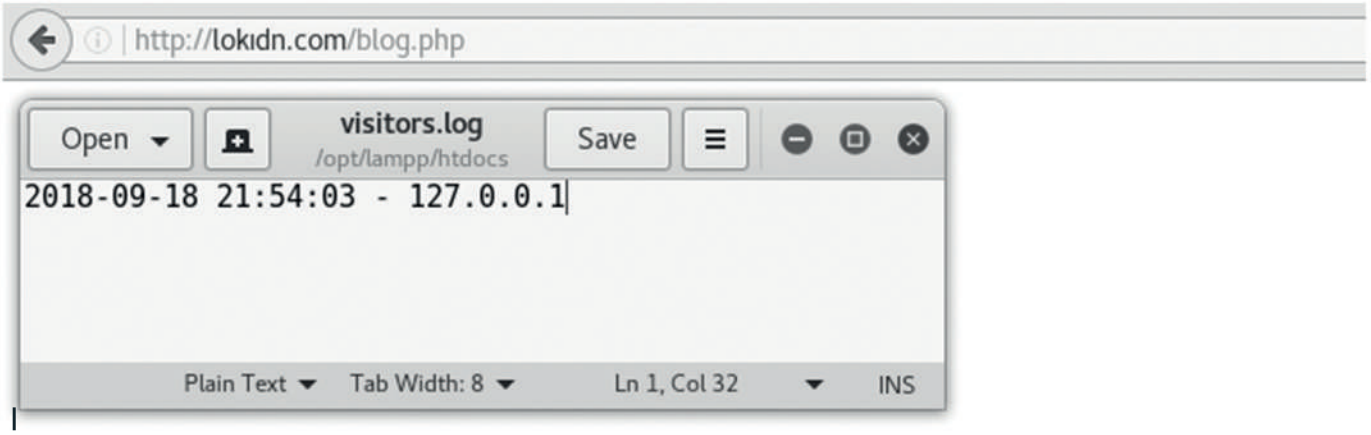
LOKIDN vulnerability can be found not only in the referenced file path links, but also in ordinary link and routing links. It is possible to make a typing error while redirecting to a different page in a different part of the web application or in the application.

```
<li><a href="http://lokıdn.com/blog.php" target="_blank">Blog</a></li>
```

When the source code of "lokidn.com" is discovered to have a LOKIDN vulnerability as above, the attacker can do many things with the "blog.php" file that will be created on the domain name "lokıdn.com". By creating a fake blog login page, the attacker can obtain user information for that application.

```
<?php
  $line = date('Y-m-d H:i:s') . " - $_SERVER[REMOTE_ADDR]";
  file_put_contents('ziyaretci.log', $line . PHP_EOL, FILE_APPEND);
?>
```

As shown above, you can create a "blog.php" file and take a look at the IP information of visitors.



If this link is also a download link at the same time, the attacker can place the file in the source code with the content that can provide remote connection such as trojan, shellcode.

The attacker can also exploit the LOKIDN vulnerability by using many phishing methods.

4.4. LOKIDN Vulnerability with Ready-Made Scripts

Many ready-made scripts and plug-ins belonging to these scripts can automatically translate any text into English or ignore special characters that it can not identify.

Such scripts do not give any errors during the translation process and they reflect the input written by the administrator with their own logic. Therefore, the administrator may not be aware of the possible LOKIDN vulnerability.

As an example, let's suppose you have typed " http:/lokıdn.com ", the custom script or plugin which is in used puts this entry into the application by translating it into "http://lokidn.com" or "http://lokdn.com". In this direction, special scripts can cause LOKIDN vulnerability.

4.5. Exploitation Mail Address Belongs To Domain Name

LOKIDN vulnerability can also occur with private mail. The developer or administrator can make a typing error while specifying the mail address as in other LOKIDN vulnerability variants. We see that an info mail link like the one below is placed on the website " lokidn.com ".

```
<li><a href="mailto:info@lokıdn.com">Contact Me</a></li>
```

The attacker can obtain private information and even personal information about the users on the site by creating an "info" e-mail address on the "lokıdn.com" domain name they have purchased.

System administrators can make keyboard errors in email addresses of administrator account in ready-made or special scripts that they use. In this case again LOKIDN vulnerability occurs. By exploiting this, the attacker can hack the system by taking the administrator account with "forget password" operations.

Even if the system administrator does not leave any LOKIDN vulnerabilities, the attacker can arrange for social engineering attacks by purchasing domain names that can be used for keyboard failure.

The attacker can hire "lokıdn.com" domain name and create an email address like "info@lokidn.com" and expect any user to make a keyboard error and send an e-mail to the fake domain name.

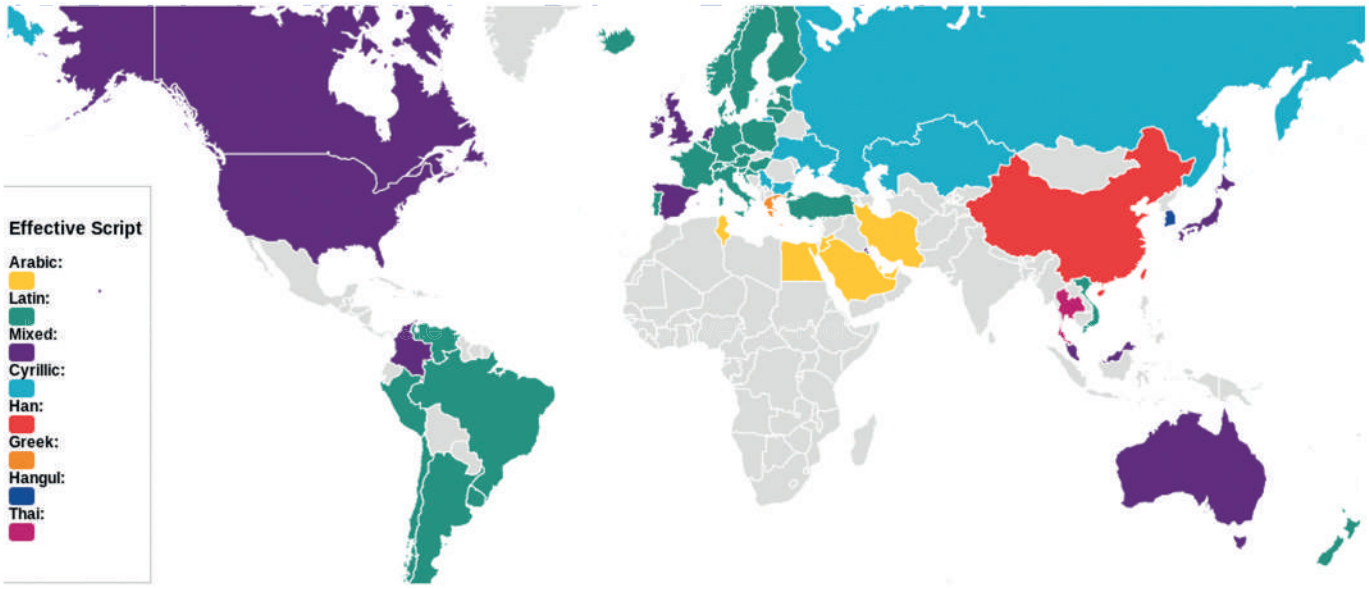
4.5. Exploitation Mail Address Belongs To Domain Name

The LOKIDN security vulnerability does not only occur by typing UNICODE characters instead of ASCII characters. If the system owner intentionally purchases the domain name "lokıdn.com" and the owner types "lokidn.com" by mistake in the source code a LOKIDN vulnerability occurs. In this case, vulnerability can also occur with reverse logic.

5.0. Analysis of Possible Situations

LOKIDN vulnerability is the result of the writing of the words used in the domain name of the people with the support of the keyboard as the main language. For example It is not possible to make a mistake for a Turkish IDN on the English keyboard. In countries where IDN service can be provided by Latin alphabet, LOKIDN vulnerability may occur if the main keyboard is used.

The IDN world map was created by The European Registry of Internet Domain Name (EURid) according to alphabet and country.



Green labeled countries use Latin alphabet. Countries with purple labeled are mixed. Therefore, it is possible LOKIDN vulnerability in these countries.

A list of characters allowed by EURID for IDN structure is provided at annex.
You can access the link at the end of the paper.

5.1. Instantiation

LOKIDN vulnerability can also occur when characters belonging to different alphabets are similar to each other.

Greece (o / o̱ - v / v̱ - α / a)	Russia (и / n / N - м / m / M - я / r / R)	Portuguese (á /a̱ - ê / é / e̱)
ονομα.com xn--mxavchb.com	имя.com xn--h1ai1d.com	olá.com xn--ol-nia.com
ονομα.com xn--v-zlb6akb.com	имr.com xn--r-otbm.com	você.com Xn--voc-hma.com
ονομα.com xn--o-zlb6adk.com	nмr.com xn--nr-8lc.com	você.com Xn--voc-dma.com

it is possible to make mistakes like all the character types.
Let's make a sample of these letters; (ì - í - ï - ı - i / ó - ȍ - ő - ǒ - ö - o)

We can use these characters for IDN. Therefore, it is possible LOKIDN vulnerability.
Example: possible to registry IDN like thats.

domaìn.com xn--doman-wsa.com	domaın.com xn--doman-q4a.com	dómain.com xn--dmain-zee.com	dőmain.com xn--dmain-hu2b.com

You can access "Homoglyph bundling tables" via *annexes*.

5.2. High-Risk IDN

The reading and spelling of the words are important in the formation of LOKIDN vulnerability. This increases the risk of LOKIDN. Because people can write as they read. For example; in Turkish, “domain” mean is “Alan Adı”. Because of that “alanadi.com” is spelling as “alanadı.com” by Turkish people. Therefore, the owner of "alanadi.com" is very likely to make a lapse of keyboard. Moreover, not only the site owner, the users can also make mistakes. This also applies to other languages.

6.0. How to Test and Protect?

Owasp ZAP, Nessus, Acunetix, Vega, Netsparker and so on. such active web scanner tools do not yet perform this vulnerability scanning and testing. After acknowledging the international validity of the LOKIDN vulnerability, the scanner tools must include the discovery and testing of this vulnerability. The vulnerability can be detected by scanning the possible IDN types in the source code of all pages and fields of the web application. When scanning is started by writing "lokidn.com " to the scanner tools, it is necessary to scan the combinations of "lokıdn.com ", " lökidn.com " and " lökıdn.com " IDN in the browser source code. It is also necessary to scan the combinations of " lokidn.com ", "lökıdn.com " and "lökidn.com" in reverse logic when scanning is started by writing " lokıdn.com " to the scanner tools.

Because there is no support for scanning tools yet, developers and administrators can analyze the source code of their system and, if used, manually scan the database for LOKIDN vulnerabilities.

Therefore, based on the risk of LOKIDN vulnerability, system owners must also lease domain names in all combinations. Otherwise, it is not possible to be exposed to LOKIDN vulnerability. Some security precautions can be taken in the used web script. If any link is entered to the input fields in the admin panel, the script should analyze this link based on the LOKIDN logic and inform the administrator with warning messages such as "Are you sure to do this?" Depending on the system administrator, these entries may be prohibited.

7.0. About me

I am a cyber security specialist. My purpose is to provide added value to the world of cyber security through the training I have given and the research I have conducted. I publish security vulnerabilities on international platforms that I have discovered.

Özkan Mustafa Akkuş (AkkuS)
Exploit-DB Author ID : 9483
Linkedin User ID : siberguvenlik
Twitter User ID : ehakkus
CTF Time User ID : 33208
Personal Blog : pentest.com.tr

8.0. Annexes

EURid IDNs the Disclosure:
https://eurid.eu/en/register-a-eu-domain/domain-names-with-special-characters-idns/

IDN Character List:
https://eurid.eu/media/filer_public/8d/18/8d18473b-ed9b-4fba-abe7-947d235f25b1/idna2008and_homoglyph_bundling_tables.pdf

IDN World Map:
https://idnworldreport.eu/maps/idn-world-map-by-script/