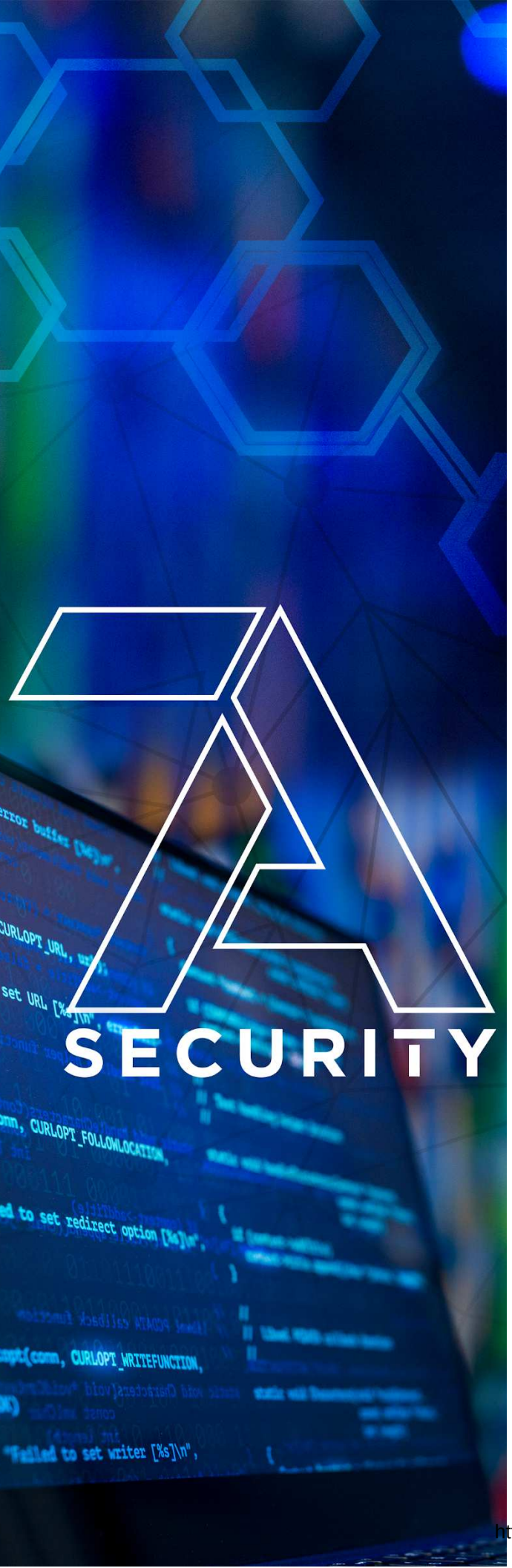

Hacking Modern Web Apps

Part: 1

Lab ID: 7

CTF

Damn Vulnerable Node App

Arbitrary File Read in sapper

Exploits for snyk.io vuln DB

7ASecurity

Protect Your Site & Apps From Attackers

admin@7asecurity.com

INDEX

Challenge #1: Damn Vulnerable Node Application **3**
Instructions 3
Installation 3

Challenge #2: Arbitrary File Read in sapper **4**
Instructions 4
Installation 4

Challenge #3: Exploits for Snyk vulnerabilities DB **5**
Instructions 5

Challenge #1: Damn Vulnerable Node Application

Instructions

Damn Vulnerable Node Application(DVNA) is an intentionally vulnerable node application which has some interesting issues, can you find them?

NOTE: Try to find the vulnerabilities by yourself first, without using Google :)

Installation

Please note all DVNA requirements are already installed in the provided lab VM, you only need to download the app itself:

Download URL:
https://training.7asecurity.com/ma/mwebapps/part1/apps/dvna-2018-11-14.zip

Alternative Download URL:
https://github.com/appsecco/dvna

If you are using the lab VM, just start DVNA like so:

Commands:

```
alert1@7ASecurity:~/vuln_node_apps/dvna$ npm start
```

Only if you are not using the lab VM, the following installation instructions might save you a bit of time:

Reference link:
https://github.com/appsecco/dvna

Step 1: Install Docker

Reference Link:
https://medium.com/@airman604/installing-docker-in-kali-linux-2017-1-fbaa4d1447fe

Commands:

```
sudo bash
apt install curl
```

```
curl -fsSL https://download.docker.com/linux/debian/gpg | apt-key add -
echo 'deb [arch=amd64] https://download.docker.com/linux/debian buster stable'
> /etc/apt/sources.list.d/docker.list
apt-get update
# Did not have it installed but ran anyway this:
apt-get remove docker docker-engine docker.io
apt-get install docker-ce
docker run hello-world
```

Once docker is installed, run the following command to start DVNA:

Command:

```
docker run --name dvna -p 9090:9090 -d appsecco/dvna:sqlite
```

Now browse to: http://localhost:9090 to interact with the app

Use the “Register a new account” option to create a user.

Email your solutions to admin@7asecurity.com for prizes

Challenge #2: Arbitrary File Read in sapper

Instructions

Sapper < 0.27.10 has an arbitrary file read vulnerability, can you find it?

NOTE: Try to find the vulnerabilities by yourself first, without using Google :)

Installation

Download the sample sapper App using the link below:

Download URL:
https://training.7asecurity.com/ma/mwebapps/part1/apps/sapper.zip

Commands:

```
unzip sapper.zip
cd my-app
npx sapper dev

# confirm the server is running
curl -vv https://localhost:3000
```

Email your solutions to admin@7asecurity.com for prizes

Challenge #3: Exploits for Snyk vulnerabilities DB

Instructions

Snyk.io maintains a list of vulnerabilities in the NPM modules. Go through the recently reported critical vulnerabilities and try to do a postmortem of why the bug existed in the first place and write exploits for the same.

URL:
https://snyk.io/vuln

NOTE: Try to find the vulnerabilities by yourself first, without looking at other people's exploits :)

Email your exploits to at least 2 different high/critical vulnerabilities (which doesn't have public exploits) from the snyk vulnerability database to admin@7asecurity.com for exclusive prizes !