Web Application Development

Alexander Menshchikov

WAD 2020 Lecture Notes – #7 «Web Security»

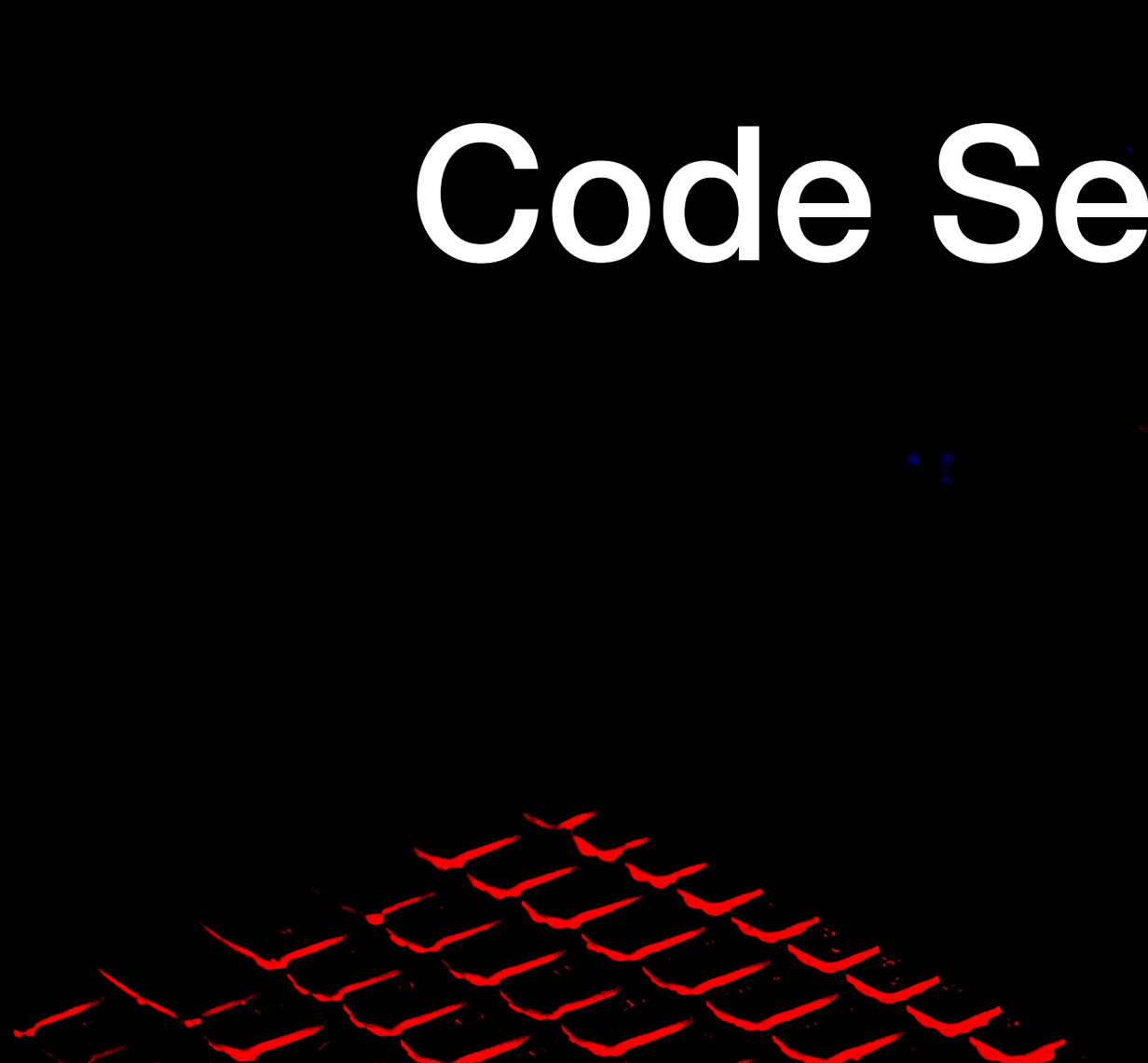
Web Security

WAD 2020 Lecture Notes – #7 «Web Security»

Web security

- 💻 Code security
- ⚖️ Paper security
- 🕸️ Environment security
- 📆 Organisational security

Code Security



Code security

- Your code
- Included code
- Data and configurations

.gitignore

```
{
  "heroku": "mongodb://admin:P12345678@ds1234.mlab.com:41952/heroku_kmd1234w?retry
Writes=false&w=majority,
  "mysql_admin": "root",
  "mysql_password": "supersecret"
}
```

Configuration file (config.json)

```
config.json
node_modules
logs
uploads
.env
```

.gitignore


```
{
  "heroku": "",
  "mysql_admin": "",
  "mysql_password": ""
}
```

Configuration file sample (config.json.sample)

.env

Branch: master ▾ | New pull request | Create new file | Upload files | Find file | Clone or download ▾

GeekaN2 Add notEmpty directive (#175) ... ✓ Latest commit 1b68800 2 days ago

.github	Add affectedUsers field (#194)	2 days ago
docker	Feature / user notifications (#192)	
migrations	Feature / user notifications (#192)	
src	Add notEmpty directive (#175)	
static	API now can host static files (#189)	
.dockerignore	Add typescript compiler (#100)	
.editorconfig	refactor: added eslint and editorconfig	
.env.sample	[Feature] Different secrets for tokens (#173)	
.eslintrc.js	Notifications support (#72)	

https://github.com/codex-team/hawk.api.nodejs

.env.sample

```
# API server port
PORT=4000

# Hawk API database URL
MONGO_HAWK_DB_URL=mongodb://mongodb:27017/hawk

# Events database URL
MONGO_EVENTS_DB_URL=mongodb://mongodb:27017/hawk_events

# JWT secret for user's refresh token
JWT_SECRET_REFRESH_TOKEN=abacaba

# JWT secret for user's access token
JWT_SECRET_ACCESS_TOKEN=belarus

# JWT secret for project's tokens (used in catcher)
JWT_SECRET_PROJECT_TOKEN=qwerty

# Tinkoff access keys
TINKOFF_TERMINAL_KEY=""
TINKOFF_SECRET_KEY=""
BILLING_DEBUG=true
BILLING_COMPANY_EMAIL="team@hawk.so"
```

Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	703	0.60
1-2	914	0.70
2-3	4880	4.00
3-4	4556	3.70
4-5	27455	22.20
5-6	23785	19.30
6-7	17054	13.80
7-8	27369	22.20
8-9	553	0.40
9-10	16185	13.10
Total	123454	

Weighted Average CVSS Score: **6.6**

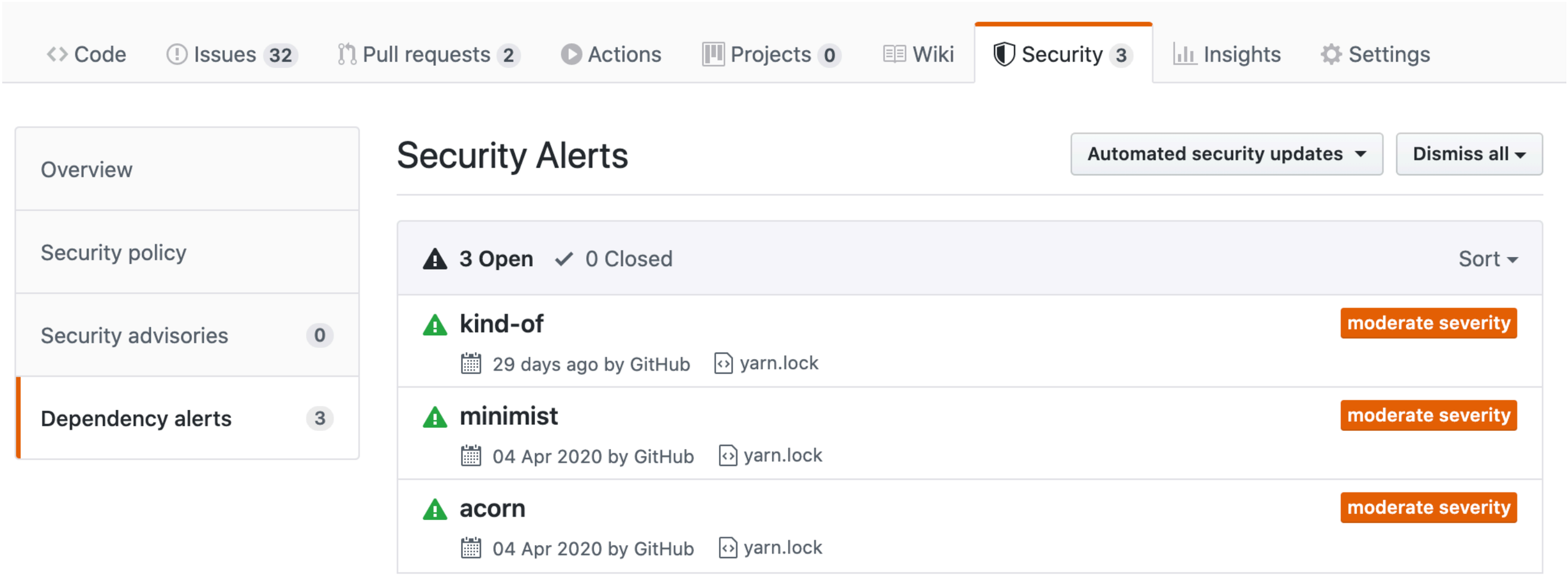
– Products Affected By CVE-2019-1010083

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	Application	Palletsprojects	Flask	0.1				Version Details Vulnerabilities
2	Application	Palletsprojects	Flask	0.2				Version Details Vulnerabilities
3	Application	Palletsprojects	Flask	0.3				Version Details Vulnerabilities
4	Application	Palletsprojects	Flask	0.3.1				Version Details Vulnerabilities
5	Application	Palletsprojects	Flask	0.4				Version Details Vulnerabilities
6	Application	Palletsprojects	Flask	0.5				Version Details Vulnerabilities
7	Application	Palletsprojects	Flask	0.5.1				Version Details Vulnerabilities
8	Application	Palletsprojects	Flask	0.5.2				Version Details Vulnerabilities
9	Application	Palletsprojects	Flask	0.6				Version Details Vulnerabilities

https://www.cvedetails.com/

https://www.cvedetails.com/cve/CVE-2019-1010083/

GitHub Security Alerts



https://help.github.com/en/github/managing-security-vulnerabilities/about-security-alerts-for-vulnerable-dependencies

Dependabot

codex-bot / github

Code | Issues 4 | Pull requests 7 | Actions | Proj

Filters | is:pr is:open

7 Open | 39 Closed | Author | Label

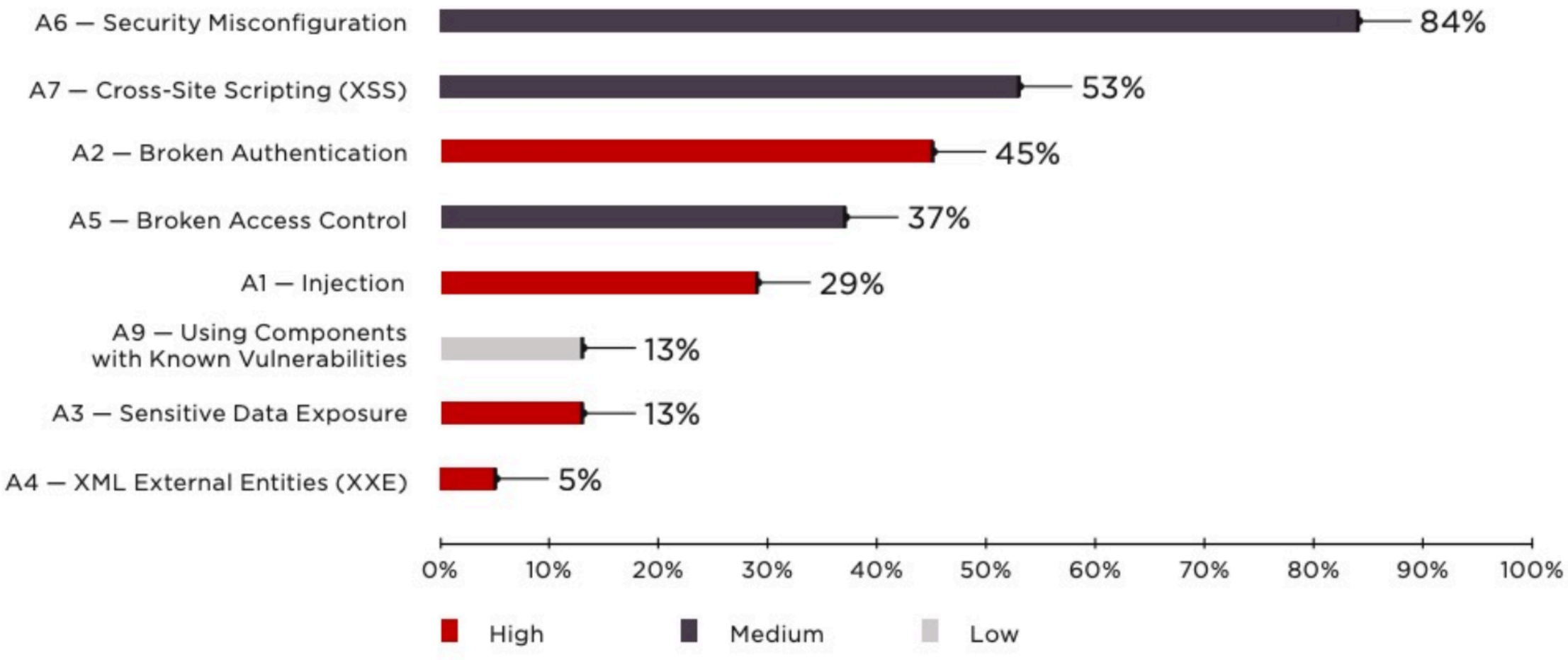
- Bump setuptools from 35.0.2 to 46.3.1 dependencies
  #76 opened 2 hours ago by dependabot-preview bot
- Bump aioamqp from 0.10.0 to 0.14.0 dependencies
  #75 opened 6 hours ago by dependabot-preview bot
- Bump wheel from 0.29.0 to 0.34.2 dependencies
  #74 opened 6 hours ago by dependabot-preview bot
- Bump aiohttp from 2.0.7 to 3.6.2 dependencies
  #73 opened 6 hours ago by dependabot-preview bot
- Bump pipdeptree from 0.10.1 to 0.13.2 dependencies
  #72 opened 6 hours ago by dependabot-preview bot
- Bump pika from 0.10.0 to 1.1.0 dependencies
  #71 opened 6 hours ago by dependabot-preview bot

```
aioamqp==0.10.0
requests
pymongo
apscheduler
aiohttp==2.0.7
asyncio==3.4.3
pika==0.10.0
pipdeptree==0.10.1
wheel==0.29.0
```

requirements.txt

OWASP

Most common vulnerabilities



https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020/

Threat analysis

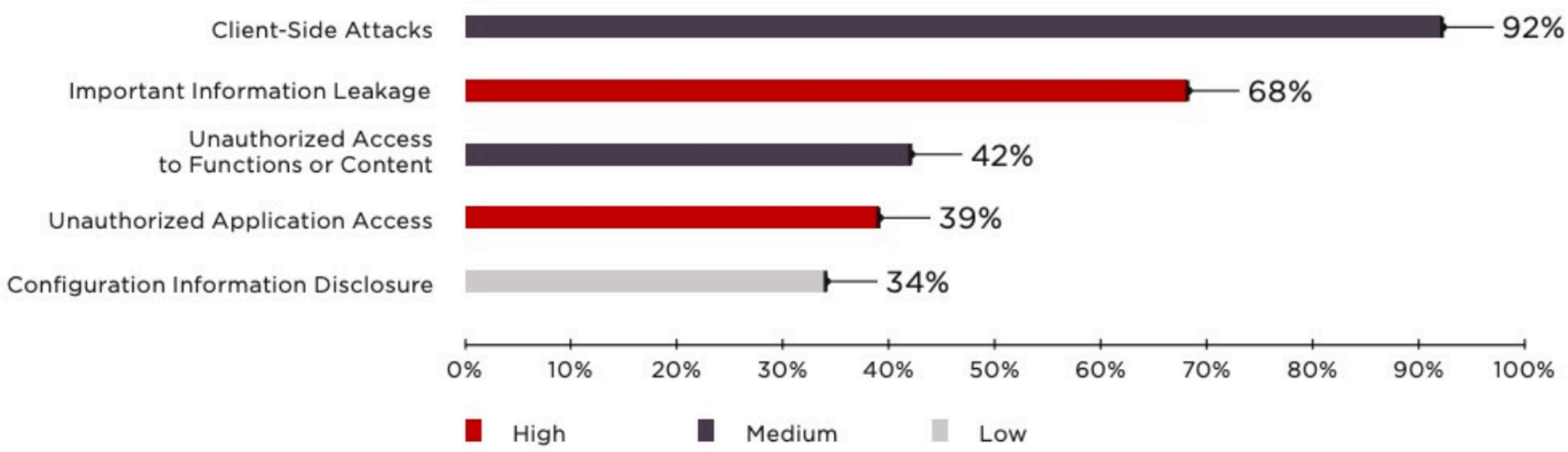


Figure 9. Top 5 most common treats (percentage of applications)

https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020/

OWASP Top 10

- Injection
- XSS

Just use common libraries

Injection

```
SELECT * FROM Users WHERE login=user AND password=pwd
```

user = «123 OR 1=1 --»

```
SELECT * FROM Users WHERE login=123 OR 1=1 -- AND password=pwd
```

```
<div>{{ input_from_user }}</div>
```

input_from_user = «<script>alert(document.cookie)</script>»

```
<div><script>alert(document.cookie)</script></div>
```

OWASP Top 10

- XXE
- Insecure Deserialization

You probably never come across

OWASP Top 10

- Broken authentication
- Sensitive Data Exposure
- Broken Access Control

Logic of your code

OWASP Top 10

- Security Misconfiguration
- Using Components with Known Vulnerabilities
- Insufficient Logging & Monitoring

DevOps

Flask Security

- Content security policy (CSP)
- HTTPS
- CSRF: https://flask-wtf.readthedocs.io/en/stable/csrf.html
- Set-Cookie options
- Headers: X-Frame-Options, X-XSS-Protection, X-Content-Type-Options

https://expressjs.com/en/advanced/best-practice-security.html

https://flask.palletsprojects.com/en/1.1.x/security/

Literature

- .gitignore: https://git-scm.com/docs/gitignore
- CVE database: https://www.cvedetails.com/
- Dependabot: https://dependabot.com/
- OWASP Top 10: https://owasp.org/www-project-top-ten/
- Cheatsheet: https://cheatsheetseries.owasp.org/
- Web security: https://developer.mozilla.org/en-US/docs/Web/Security
- Flask security: https://flask.palletsprojects.com/en/1.1.x/security/
- Cookie security: https://web.dev/samesite-cookies-explained/

Paper Security

Paper security

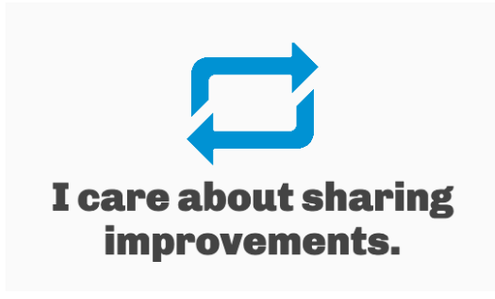
- All about licences

- Protect your code from reuse

- Protect yourself from legal issues

GitHub license

- Apache License 2.0
- GNU General Public License v3.0
- MIT License



No license :(

When you make a creative work (which includes code),

the work is under exclusive copyright by default.

...

nobody else can copy, distribute, or modify your work

...

on GitHub, you have accepted the Terms of Service, by which you allow others to view and fork your repository

...

Although a code host such as GitHub may allow you to view and fork the code, this does not imply that you are permitted to use, modify, or share the software for any purpose.

https://choosealicense.com/no-permission/

GitHub license

codex-team / capella

Unwatch 25 | Unstar 69 | Fork 12

Code | Issues 14 | Pull requests 0 | Actions | Security 0 | Insights | Settings

Cloud service for image storage and delivery https://capella.pics/ Edit

cloud-service pictures api image-storage filter crop-image resize-images capella codex open-source Manage topics

521 commits | 3 branches | 0 packages | 10 releases | 12 contributors | MIT

codex-team / editor.js

Sponsor | Used by 543 | Unwatch 174 | Unstar 11.8k | Fork 720

Code | Issues 195 | Pull requests 16 | Actions | Projects 0 | Security 1 | Insights | Settings

A block-styled editor with clean JSON output https://editorjs.io Edit

editor wysiwyg redactor codex-editor javascript typescript ui json raw-data Manage topics

518 commits | 34 branches | 0 packages | 6 releases | 1 environment | 15 contributors | Apache-2.0

Choose license

- Apache License 2.0

Permissions
- ✓ Commercial use
- ✓ Modification
- ✓ Distribution
- ✓ Patent use
- ✓ Private use

Limitations
- ✗ Trademark use
- ✗ Liability
- ✗ Warranty

Conditions
- ⓘ License and copyright notice
- ⓘ State changes

- GNU General Public License v3.0

Permissions
- ✓ Commercial use
- ✓ Modification
- ✓ Distribution
- ✓ Patent use
- ✓ Private use

Limitations
- ✗ Liability
- ✗ Warranty

Conditions
- ⓘ License and copyright notice
- ⓘ State changes
- ⓘ Disclose source
- ⓘ Same license

- MIT License

Permissions
- ✓ Commercial use
- ✓ Modification
- ✓ Distribution
- ✓ Private use

Limitations
- ✗ Liability
- ✗ Warranty

Conditions
- ⓘ License and copyright notice

Literature

- Choose license: https://choosealicense.com/
- GitHub licenses: https://help.github.com/en/github/creating-cloning-and-archiving-repositories/licensing-a-repository
- In simple words: https://tldrlegal.com/license/mit-license

Environment Security

Environment security

- Configuration hardening
- Logging and monitoring
- Intrusion detection and prevention

Firewall

- Find listening ports

```
netstat -tulpn
```

- Uncomplicated Firewall

```
ufw allow 22      ufw allow 80          ufw allow 443

ufw enable        ufw status verbose    ufw disable
```

```
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), deny (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
443                        ALLOW IN    Anywhere
80                         ALLOW IN    Anywhere
22022                      ALLOW IN    Anywhere
443 (v6)                   ALLOW IN    Anywhere (v6)
80 (v6)                    ALLOW IN    Anywhere (v6)
22022 (v6)                 ALLOW IN    Anywhere (v6)
```

Nginx logging

```
server {
    listen       80;
    server_name  localhost;

    access_log /var/log/nginx/access.log;
    error_log /var/log/nginx/error.log;

    location / {
        proxy_pass http://flask-simple:5000/;
    }
}
```

```
37.49.230.229 - - [15/May/2020:14:43:53 +0000] "POST /cgi-bin/
ViewLog.asp HTTP/1.1" 400 0 "-" "python-requests/2.20.0" "-"
188.37.65.2 - - [15/May/2020:16:00:24 +0000] "POST /cgi-bin/
ViewLog.asp HTTP/1.1" 400 0 "-" "python-requests/2.20.0" "-"
94.19.207.227 - - [15/May/2020:16:30:49 +0000] "GET /HNAP1/ HTTP/1.1"
404 232 "http://31.184.255.217:8080/" "Mozilla/5.0 (Windows NT 5.1;
rv:9.0.1) Gecko/20100101 Firefox/9.0.1" "-"
```

Docker logging

- Show docker-compose logs

```
docker-compose logs
```

- Show docker logs

```
docker ps
```

```
docker logs <CONTAINER_ID> -f
```

SSH hardening

- Change port in **/etc/ssh/sshd_config** to random

```
Port 17384
```

- Create SSH key and place it to ~/.ssh/authorized_keys
- Create SSH config **~/.ssh/config** on your laptop (example):

```
Host wad
    HostName 31.184.255.217
    Port 22022
    User root
    IdentityFile ~/.ssh/id_rsa
```

- Use **ssh wad** CLI command to connect

Fail2ban

- Find listening ports

  ```
  apt-get install fail2ban
  ```

- Add **enabled = true** to /etc/fail2ban/jail.conf and restart

  ```
  service fail2ban restart
  ```

- Show stats

  ```
  fail2ban-client status

  fail2ban-client status sshd
  ```

Fail2ban

```
[sshd]

# To use more aggressive sshd
# normal (default), ddos, ext
# See "tests/files/logs/sshd"
#mode   = normal
enabled = true
maxretry = 3
port    = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s
```

/etc/fail2ban/jail.conf

```
root@cs785268:~# fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
root@cs785268:~# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     8
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   95.213.200.245
```

SSH protection enabled
Banned one IP

Literature

- UFW: https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-with-ufw-on-ubuntu-18-04

- Nginx logs: https://www.journaldev.com/26756/nginx-access-logs-error-logs

- Docker logs: https://docs.docker.com/engine/reference/commandline/logs/

- SSH setup: https://www.digitalocean.com/community/tutorials/how-to-set-up-ssh-keys-on-ubuntu-1804

- Fait2ban setup: https://www.techrepublic.com/article/how-to-install-fail2ban-on-ubuntu-server-18-04/

Organisational security

Organisational security

- Security audit

- Automated security checking

Literature

- Vulnerability scanners: https://www.acunetix.com/

- Nmap: https://securitytrails.com/blog/nmap-vulnerability-scan

Teams

Team 1	Time picker	https://github.com/itmo-wad/time-picker
Team 2	📆🙋‍♂️ Who when can	https://github.com/itmo-wad/Who_when_can
Team 3	🔄🍕 Ur-opinion	https://github.com/itmo-wad/Ur-opinion
Team 4	📝☁️ CommentCloud	https://github.com/itmo-wad/CommentCloud
Team 5	🧸❓ Cozy quiz	https://github.com/itmo-wad/Cozy_quiz
Team 6	🇨🇭🔪 Swiss knife	https://github.com/itmo-wad/Swiss-knife
Team 7	😄⛏️ Emoji picker	https://github.com/itmo-wad/Emoji-picker

!?

Quiz time

https://quiz.itmo.xyz/

Practice time