Web Security

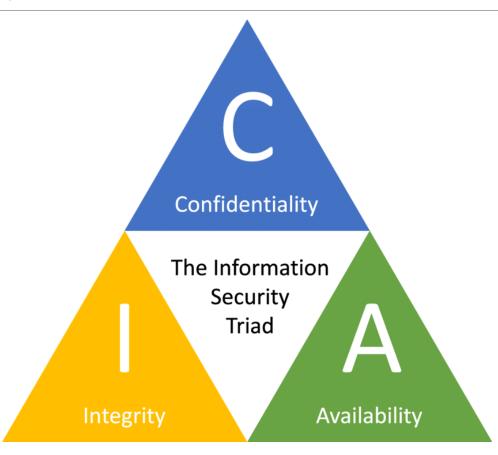
What is Web App Security?



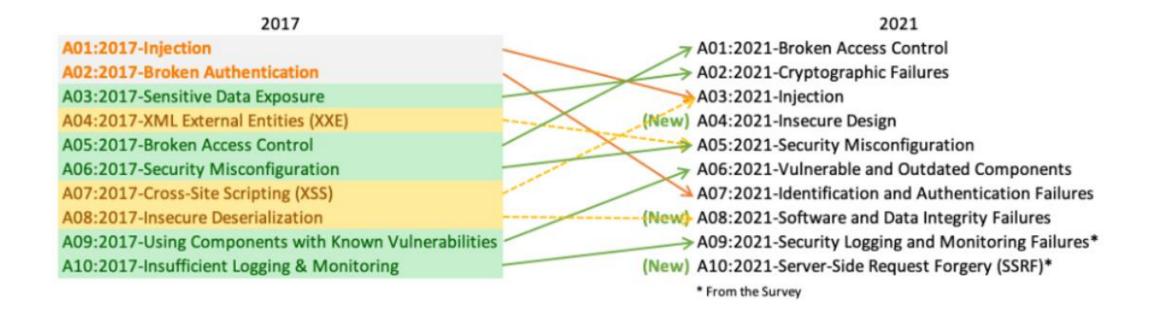
Why is web security testing important?



Security key



OWASP Top Ten



A03: Injection – SQLin & XSS

```
m.orgmanager.handlers.RequestMandlers.
app/page/analyze webparans and according to the second sec
     8249868e-afd8-46ac-9745-839146a20f09".
    115":"36"}{"timestamp":"2017-06-03718:43:331
    "file=chartdata_new.json", "class"| "com.orgmonager
      "14402n620jm9trnd3s3m7wg@k", "sizeChars": 48455"
     illis": "0", "level": "INFO", "weburt": "/app/page/report
       "789d89cb-bfa8-4e7d-8847-498454af885d", "SessionID": "34402no.
     lis":"7"}{"timestamp":"2017-06-03T18:46:921.000", "deltasta
       organager.handlers.RequestHandler", "method": "handle", "reques
        "10190", "message": "Duration Log", "durationmillis": "10")("times
       pp/rest/json/file", "webParams": "filenchartdata_new.json", "closs
         '7ac6ce95-19e2-4a68-88d7-6ead86e273d1", "sessionID"; "ledozna
```

Tools



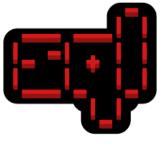












Tools: NMAP



Host discovery

Service detection

Operating system detection

TCP/UDP scan

Login credentials brute force

Tools: SkipFish



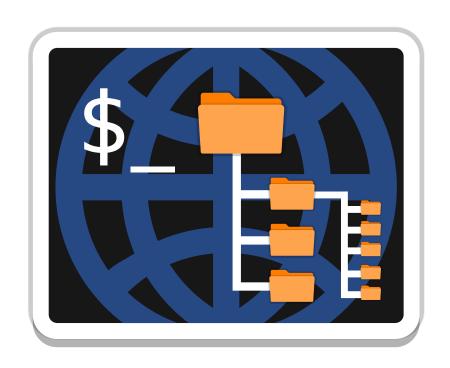
Open source

Fully automated

Large number of modules

Enumeration

Tools: dirb

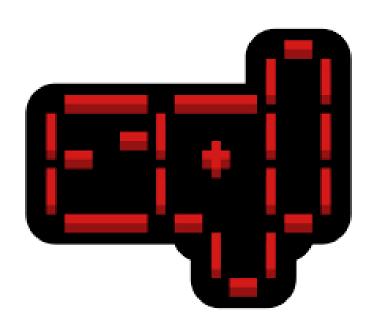


Dictionary based

Preconfigured attack wordlists

Used by professionals

Tools: SQLmap



Support popular database engines

Support multiple injection techniques

Software fingerprinting

Support password hash crack

Support to download and upload any file from db

Exploits & CVE

https://www.exploit-db.com/

https://www.vulnerability-lab.com

https://vuldb.com/

https://cve.mitre.org/

https://www.cvedetails.com/

https://nvd.nist.gov/

Practical Example

The application is available at:

https://github.com/PiotrKontowicz/ExampleSQL

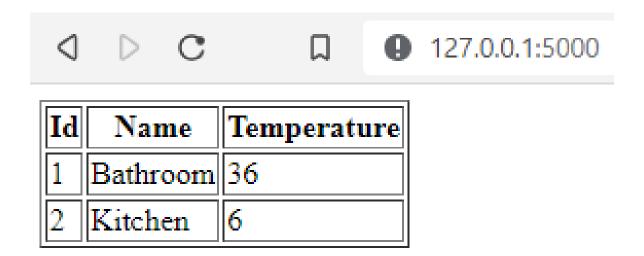
Endpoints:

ohttp://127.0.0.1:5000/

ohttp://127.0.0.1:5000/name

ohttp://127.0.0.1:5000/save

http://127.0.0.1:5000/



http://127.0.0.1:5000/name



Id	Name	Temperature
1	Bathroom	24

http://127.0.0.1:5000/save

ok

Example payloads:

1);DROP TABLE#

- 1),('hacker',-100)#
- OBathroom' UNION SELECT table_name, null, null FROM information_schema.tables where table_schema ='test_app'#
- **OBathroom' UNION SELECT id, name, NULL from admins#**

How to prevent SQLin?

Do not use data from any input directly to create SQL query, like this:

```
'SELECT * FROM data where name=\'{}\''.format(name)
```

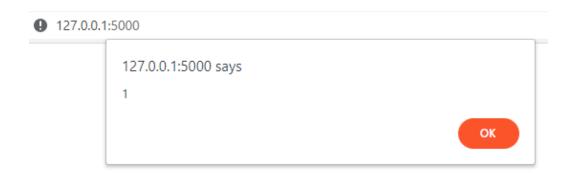
Or this:

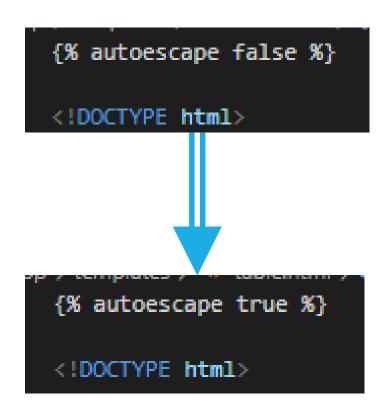
```
'SELECT * FROM data where name=\'' + name +'\''
```

Use parameterized query or prepared statements:

- <u>ohow-and-why-to-use-parameterized-queries</u>
- ohow-to-prevent-sql-injection-vulnerabilities-how-prepared-statements

XSS





Additional resources:

https://tryhackme.com/

https://portswigger.net/web-security

https://academy.hackthebox.com/

https://cryptohack.org/

https://www.hacker101.com/

Thank You!

For Your Attention

Piotr Kontowicz piotr.kontowicz@put.poznan.pl