



GeekTalks

Tema:
JavaScript
#geekspaceit



**Web is Secure
Let's Hack It.**

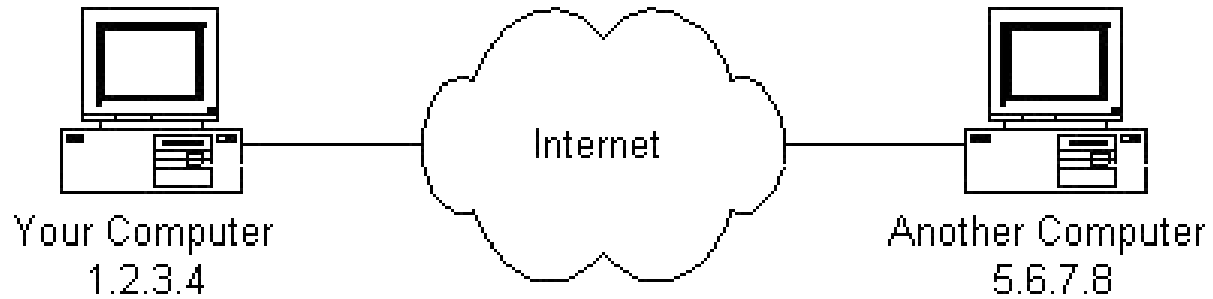


Ihor Kaminnyi

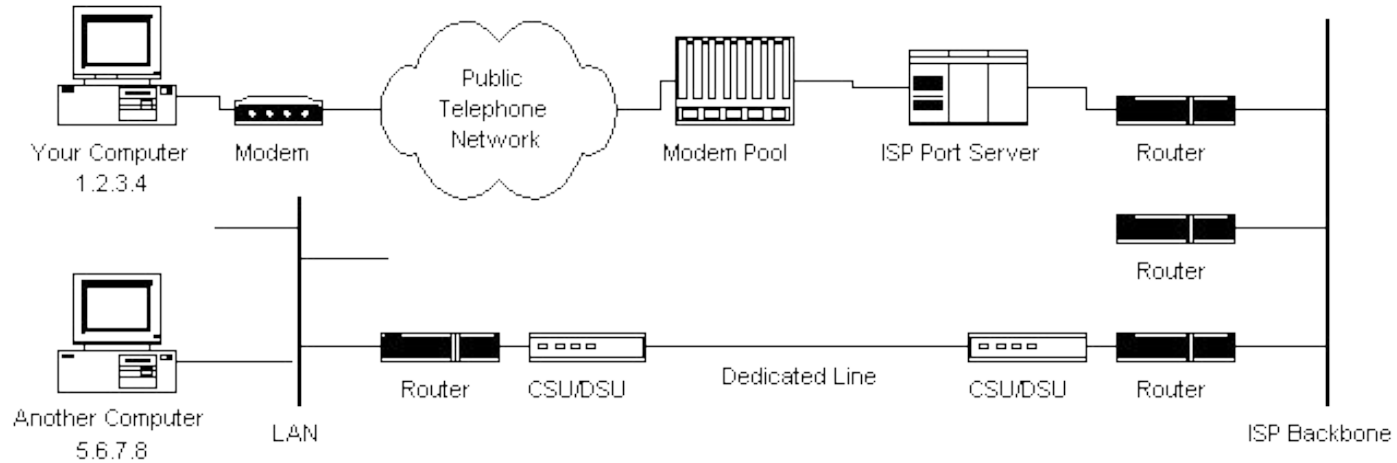
Front-end developer



How internet works ?



How internet works ?

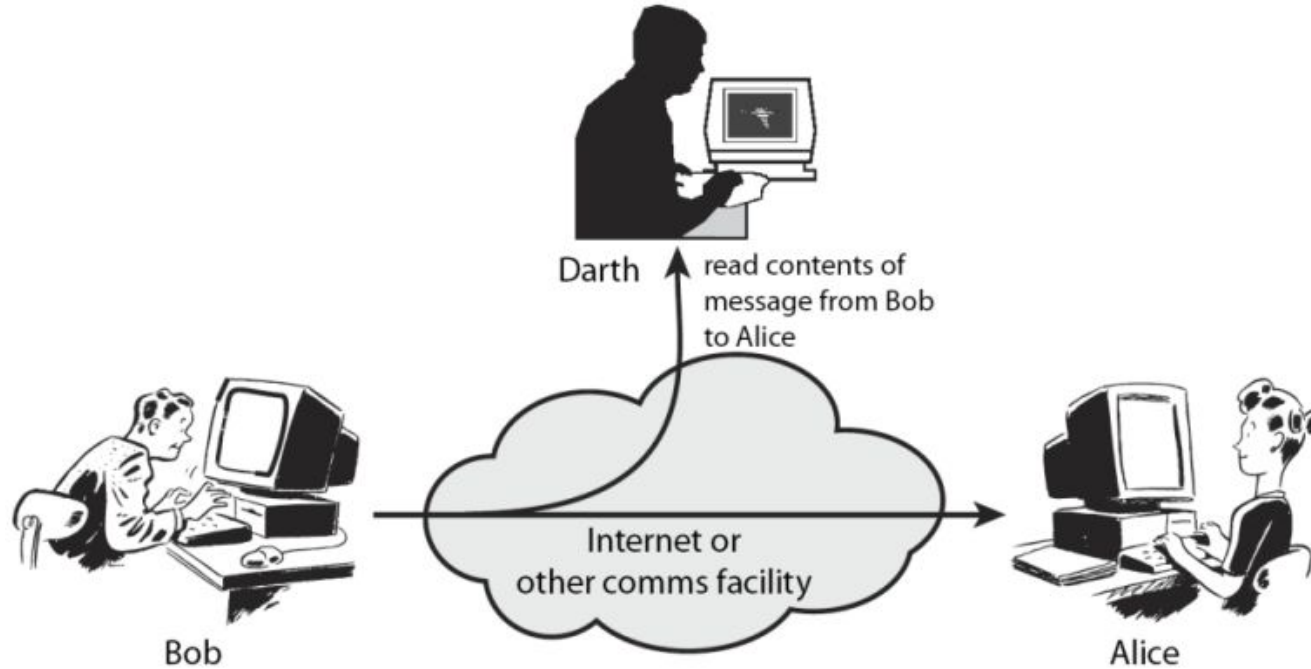


Check route for your request

igorkaminnyy — -bash — 145x35

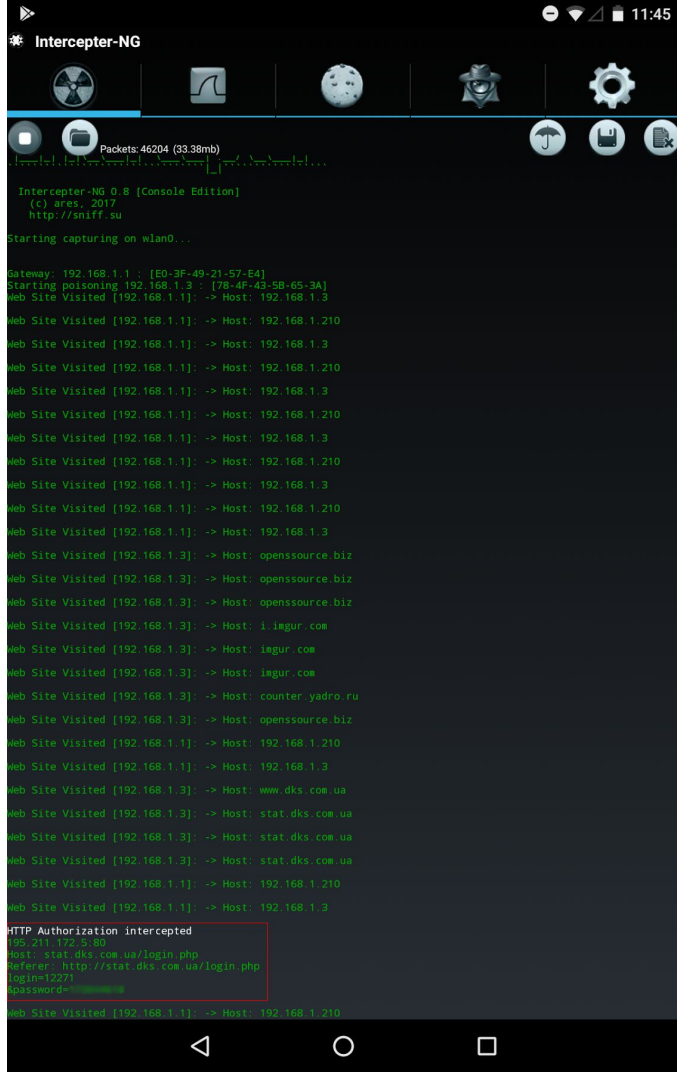
```
MBP-Igor:~ igorkaminnyy$ traceroute www.viseven.com
traceroute to www.viseven.com (136.243.6.189), 64 hops max, 52 byte packets
 1  router.asus.com (192.168.1.1)  1.634 ms  1.205 ms  1.224 ms
 2  ns2.dks.com.ua (195.211.172.21)  1.721 ms  1.732 ms  1.674 ms
 3  bgp-rt.dks.com.ua (195.211.172.1)  2.005 ms  2.211 ms  1.945 ms
 4  host49-223.impuls.net.ua (195.69.223.49)  1.921 ms  1.936 ms  2.084 ms
 5  194.44.35.245 (194.44.35.245)  4.944 ms  4.666 ms  5.480 ms
 6  194.44.212.254 (194.44.212.254)  11.327 ms  12.178 ms  13.063 ms
 7  decix2-gw.hetzner.de (80.81.193.164)  42.521 ms  41.303 ms  41.177 ms
 8  core24.fsn1.hetzner.com (213.239.203.150)  52.070 ms
   core23.fsn1.hetzner.com (213.239.229.74)  46.013 ms
   core24.fsn1.hetzner.com (213.239.203.150)  46.070 ms
 9  ex9k1.dc12.fsn1.hetzner.com (213.239.203.174)  45.163 ms
   ex9k1.dc12.fsn1.hetzner.com (213.239.203.186)  47.234 ms
   ex9k1.dc12.fsn1.hetzner.com (213.239.203.174)  45.620 ms
10  static.189.6.243.136.clients.your-server.de (136.243.6.189)  45.313 ms  46.074 ms  45.813 ms
MBP-Igor:~ igorkaminnyy$
```

Man in the middle attack (MITM)



Popular tools for MITM attack





Demo MITM: Interceptor-ng

```
HTTP Authorization intercepted
195.211.172.5:80
Host: stat.dks.com.ua/login.php
Referer: http://stat.dks.com.ua/login.php
login=12271
&password=12345678
```

XSS

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites.

① 192.168.1.15/bWAPP/xss_get.php?firstname=Fedya&lastname=<script>alert(document.cookie)</script>&form=submit

Подтвердите действие на 192.168.1.15:

PHPSESSID=ed92fe0074c0e1004919d6c31e2118e0; security_level=0

OK

XSS

/ XSS - stored (Blog) /

I'm fine! <script>alert(document.cookie)</script>

Submit

Add:

Show all:

Delete:

Your entry was added to our blog!

#	Owner	Date	Entry
2	bee	2017-09-19 21:13:30	Hi guys!!!!
3	bee	2017-09-19 21:13:39	How are you?

XSS

/ XSS - stored (Blog) /

Submit

Add:

Show all:

Delete:

Your entry

```
PHPSESSID=d1a07588615e95ece48346f43b29711f;  
security_level=0
```

[Закреть](#)

#	Owner	Date	Entry
2	bee	2017-09-19 21:13:30	Hi guys!!!!
3	bee	2017-09-19 21:13:39	How are you?
4	bee	2017-09-19 21:14:38	I'm fine!

XSS

192.168.1.15/bWAPP/xss_get.php?firstname=Fedya&lastname=<script>alert(document.cookie)</script>&form=submit



Страница недоступна

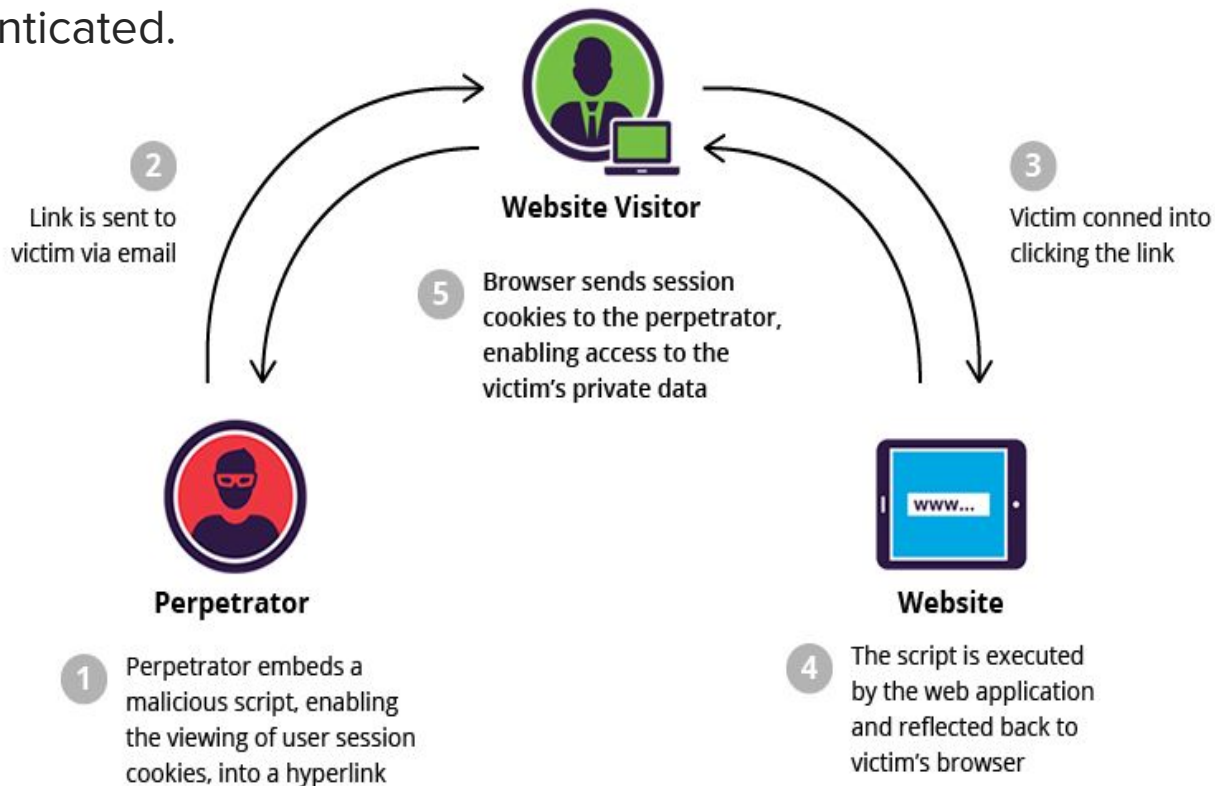
Браузер Chrome обнаружил на этой странице необычный код и заблокировал его, чтобы защитить ваши данные (например, пароли, а также номера телефонов и банковских карт).

Попробуйте [открыть главную страницу сайта](#).

ERR_BLOCKED_BY_XSS_AUDITOR

CSRF

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated.



CSRF

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated.

/ CSRF (Transfer Amount) /

Amount on your account: **1000 EUR**

Account to transfer:

Amount to transfer:

CSRF

192.168.1.15/bWAPP/csrf_2.php?account=123-45678-90&amount=100&action=transfer



/ CSRF (Transfer Amount) /

Amount on your account: **900 EUR**

Account to transfer:

Amount to transfer:

CSRF

/ HTML Injection - Stored (Blog) /

Nice to see you!

```

```

Submit

Add:

Show all:

Delete:

#	Owner	Date	Entry
2	bee	2017-09-19 21:13:30	Hi guys!!!!
3	bee	2017-09-19 21:13:39	How are you?
4	bee	2017-09-19 21:14:38	I'm fine!

CSRF

/ CSRF (Transfer Amount) /

Amount on your account: **-1100 EUR**

Account to transfer:

Amount to transfer:

How vulnerabilities works ?

<http://www.itsecgames.com>

bwAPP
an extremely buggy web app !

Home Bugs Download Talks & Training Blog

/ Home /

bwAPP, or a *buggy web application*, is a free and open source deliberately insecure web application. It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities. bwAPP prepares one to conduct successful penetration testing and ethical hacking projects.

What makes bwAPP so unique? Well, it has over **100 web vulnerabilities!** It covers all major known web bugs, including all risks from the OWASP Top 10 project.

bwAPP is a PHP application that uses a MySQL database. It can be hosted on Linux/Windows with Apache/IIS and MySQL. It can also be installed with WAMP or XAMPP.

Another possibility is to download the *bee-box*, a custom Linux VM pre-installed with bwAPP.

Download our **What is bwAPP?** introduction tutorial, including free exercises...

bwAPP is for web application security-testing and educational purposes only. Have fun with this free and open source project!

Cheers, Malik Mesellem

bwAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive *framing*?

Choose your bug:

- ✓ ----- bwAPP v2.2 -----
- / A1 - Injection /
- HTML Injection - Reflected (GET)
- HTML Injection - Reflected (POST)
- HTML Injection - Reflected (Current URL)
- HTML Injection - Stored (Blog)
- iFrame Injection
- LDAP Injection (Search)
- Mail Header Injection (SMTP)
- OS Command Injection
- OS Command Injection - Blind
- PHP Code Injection
- Server-Side Includes (SSI) Injection
- SQL Injection (GET/Search)
- SQL Injection (GET/Select)
- SQL Injection (POST/Search)
- SQL Injection (POST/Select)
- SQL Injection (AJAX/JSON/jQuery)
- SQL Injection (CAPTCHA)
- SQL Injection (Login Form/Hero)
- SQL Injection (Login Form/User)
- SQL Injection (SQLite)
- SQL Injection (Drupal)
- SQL Injection - Stored (Blog)
- SQL Injection - Stored (SQLite)
- SQL Injection - Stored (User-Agent)
- SQL Injection - Stored (XML)
- SQL Injection - Blind - Boolean-Based
- SQL Injection - Blind - Time-Based
- SQL Injection - Blind (SQLite)
- SQL Injection - Blind (Web Services/SOAP)
- XML/XPath Injection (Login Form)
- XML/XPath Injection (Search)
- /
- / A2 - Broken Auth. & Session Mgmt. /
- Broken Authentication - CAPTCHA Bypassing
- Broken Authentication - Forgotten Function
- Broken Authentication - Insecure Login Forms
- Broken Authentication - Logout Management

Where i can read about vulnerabilities ?



Common Vulnerabilities and Exposures (CVE®) is a list of common identifiers for publicly known cyber security vulnerabilities.



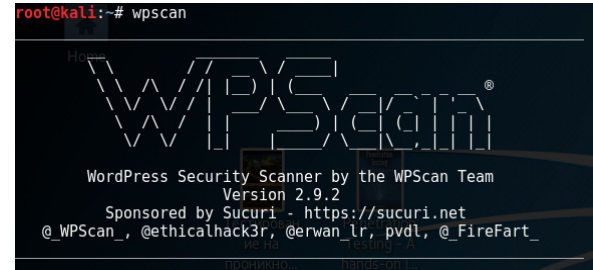
The **Exploit Database** – ultimate archive of **Exploits**, **Shellcode**, and **Security Papers**.

How i can protect my project ?
Vulnerability Scanners:



How i can protect my project ?

Vulnerability Scanners:



File Edit View Search Terminal Help

```
[!] Title: WordPress 2.5.0-4.7.4 - Filesystem Credentials Dialog CSRF
Reference: https://wpvulndb.com/vulnerabilities/8818
Reference: https://wordpress.org/news/2017/05/wordpress-4-7-5/
Reference: https://github.com/WordPress/WordPress/commit/38347d7c580be4cdd8476e4bbc653d5c79ed9b67
Reference: https://sumofpwn.nl/advisory/2016/cross_site_request_forgery_in_wordpress_connection_information.html
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9064
[i] Fixed in: 4.7.5

[!] Title: WordPress 3.3-4.7.4 - Large File Upload Error XSS
Reference: https://wpvulndb.com/vulnerabilities/8819
Reference: https://wordpress.org/news/2017/05/wordpress-4-7-5/
Reference: https://github.com/WordPress/WordPress/commit/8c7ea71edbbffca5d9766b7bea7c7f3722ffafa6
Reference: https://hackerone.com/reports/203515
Reference: https://hackerone.com/reports/203515
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9061
[i] Fixed in: 4.7.5

[!] Title: WordPress 3.4.0-4.7.4 - Customizer XSS & CSRF
Reference: https://wpvulndb.com/vulnerabilities/8820
Reference: https://wordpress.org/news/2017/05/wordpress-4-7-5/
Reference: https://github.com/WordPress/WordPress/commit/3d10fef22d788f29aed745b0f5ff6f6baea69af3
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9063
[i] Fixed in: 4.7.5
```

Where i can read about vulnerabilities ?

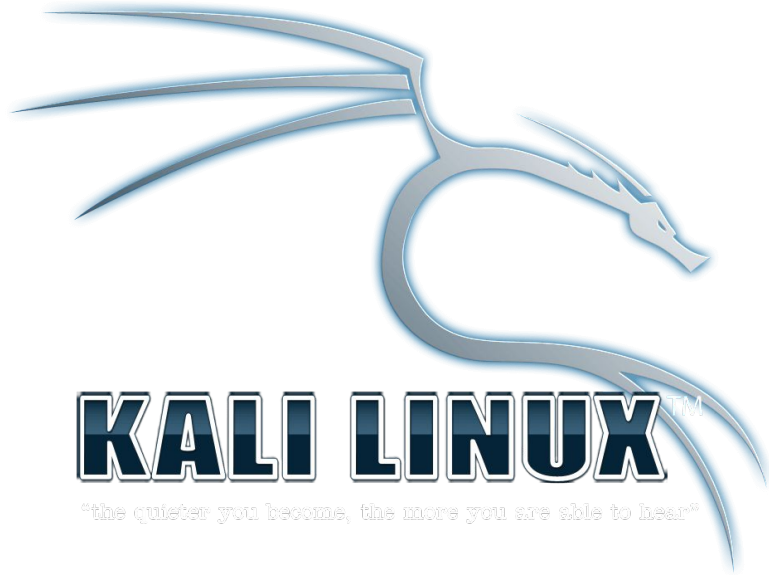


OWASP

Open Web Application
Security Project

The **Open Web Application Security Project** (OWASP) is a worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations are able to make informed decisions.

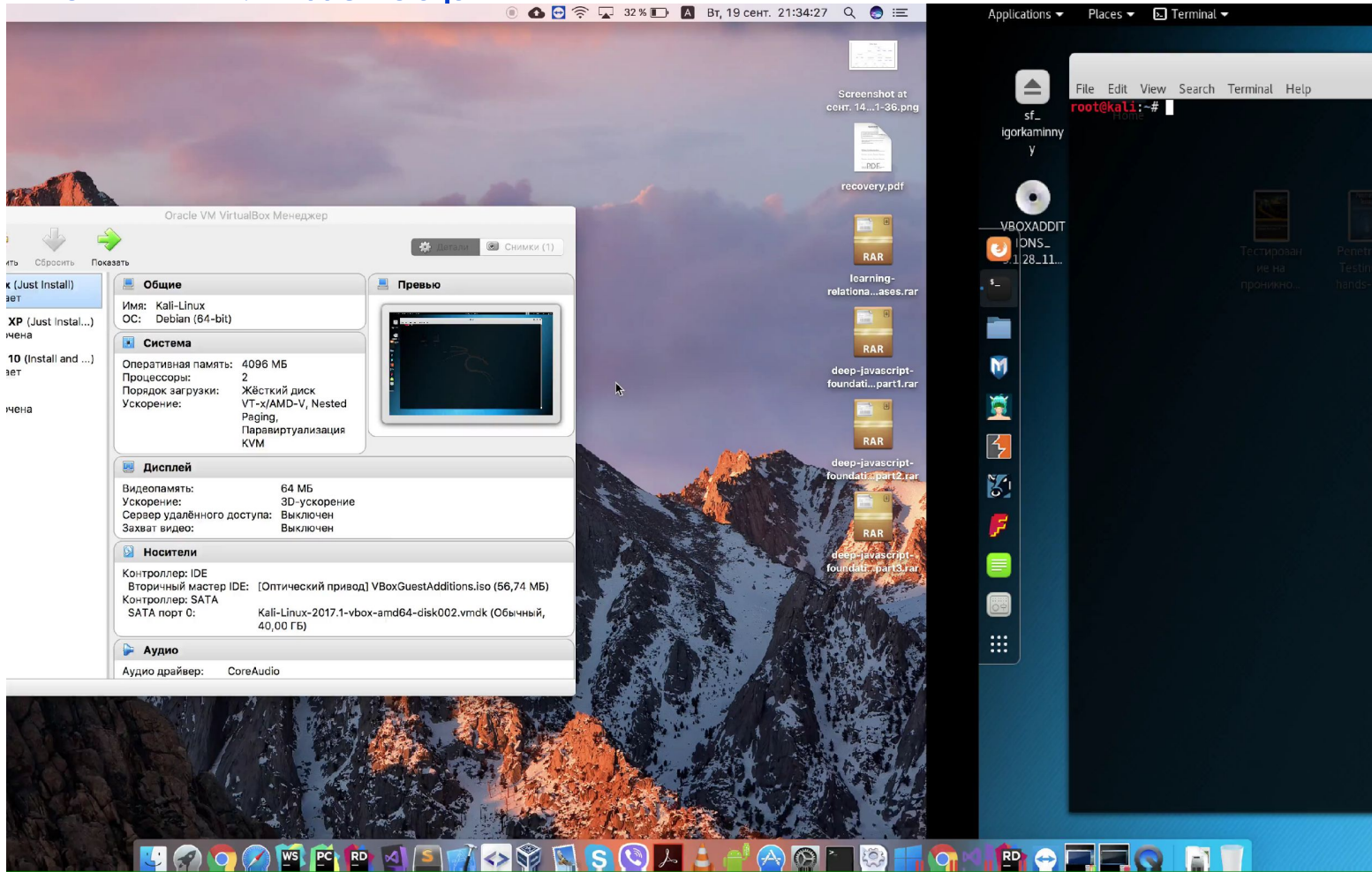
How to get started ?



Useful links:

- How the Internet works ? (goo.gl/CpXm28)
- OWASP top 10 (goo.gl/Qw7RKH)
- Angular 1.6 - Expression Sandbox Removal (goo.gl/F8oezb)
- Vulnerability Scanning Tools (goo.gl/0F3IT)
- Kali Linux home (goo.gl/5PBBkn)
- bwapp (goo.gl/qWDiLC)
- Learn To Hack (goo.gl/J5S5hC)

Demo MITM: Ettercap



Как часто вы обновляете свои веб-приложения?

С какими уязвимостями вы сталкивались?

Используете ли вы VPN?

Есть ли в вашей организации должность специалиста по безопасности?