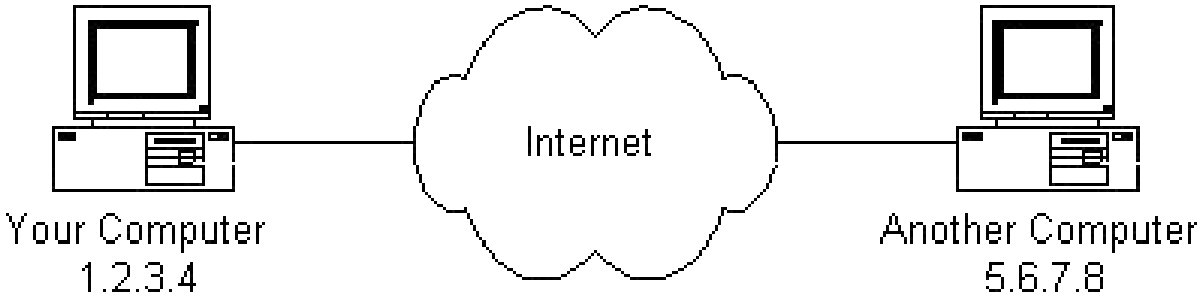

Geek_Space
GeekTalks
Tema:
JavaScript
#geekspaceit

Web is Secure
Let's Hack It.

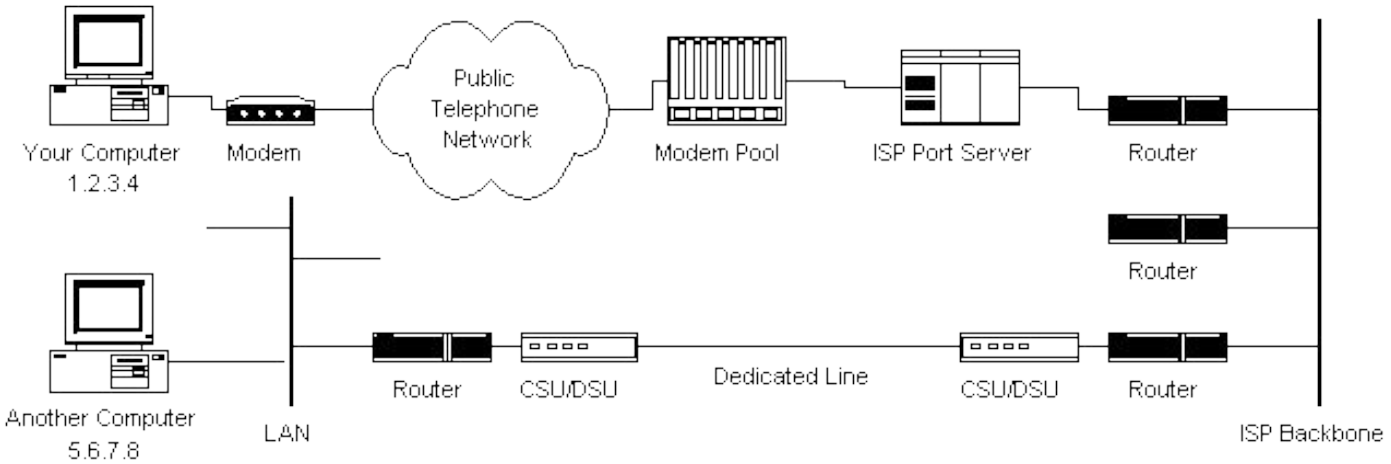
Ihor Kaminnyi

Front-end developer

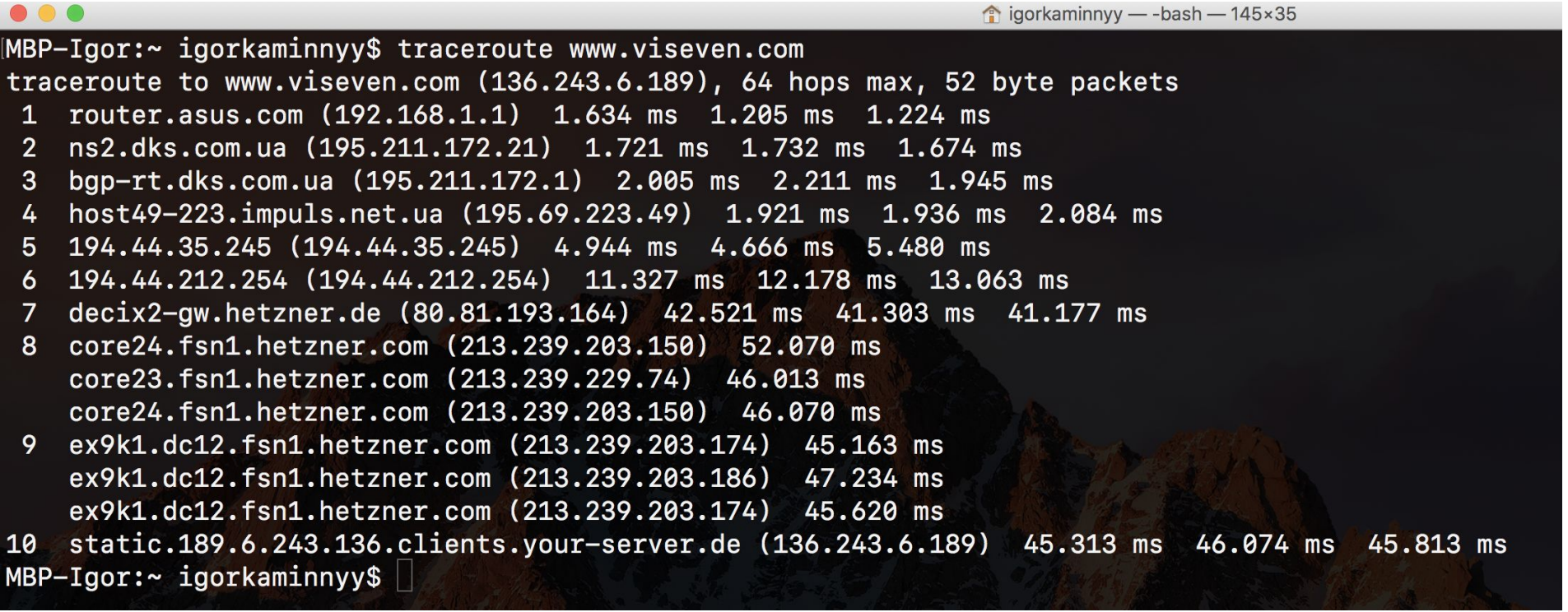
How internet works ?



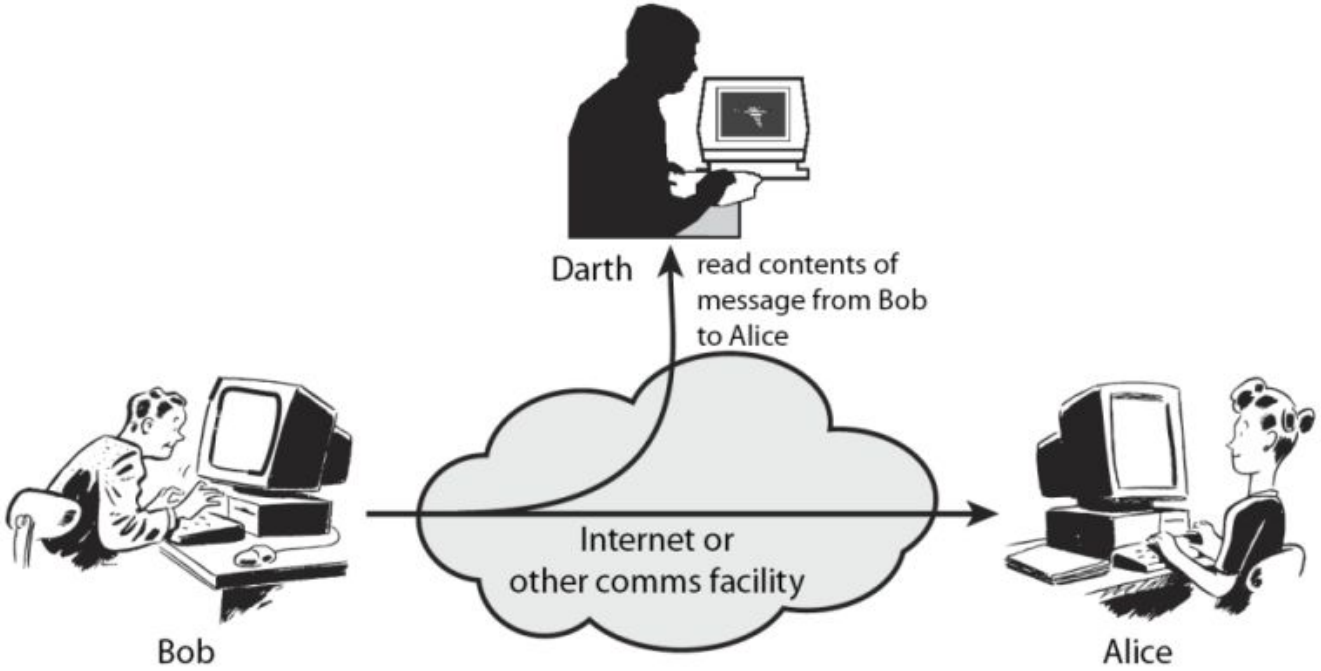
How internet works ?



Check route for your request

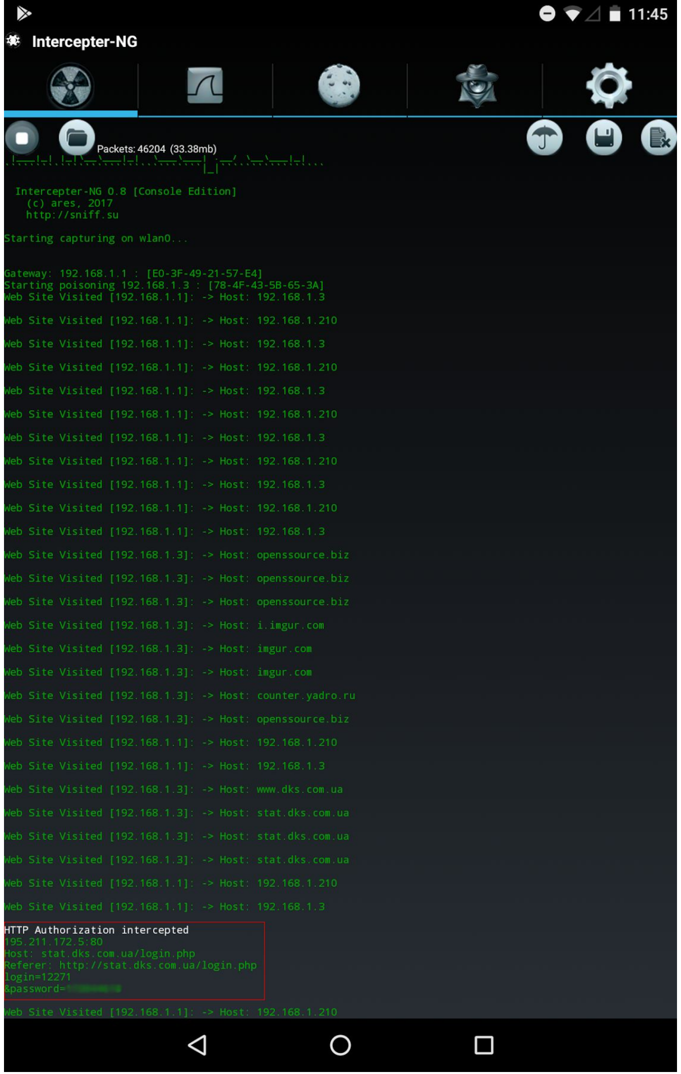


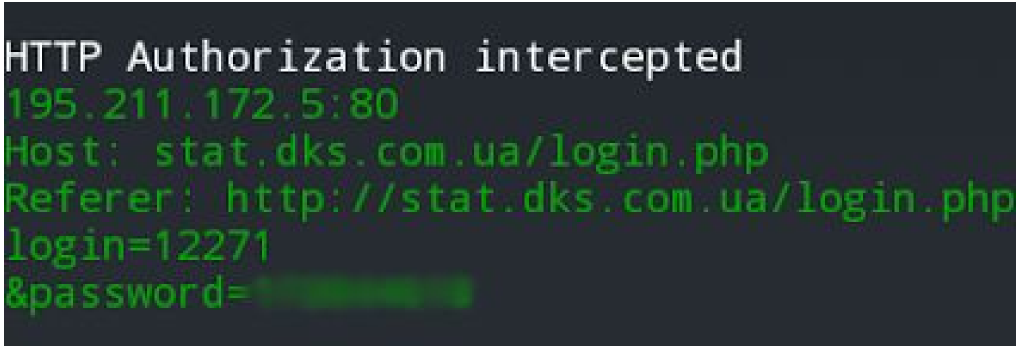
Man in the middle attack (MITM)



Popular tools for MITM attack

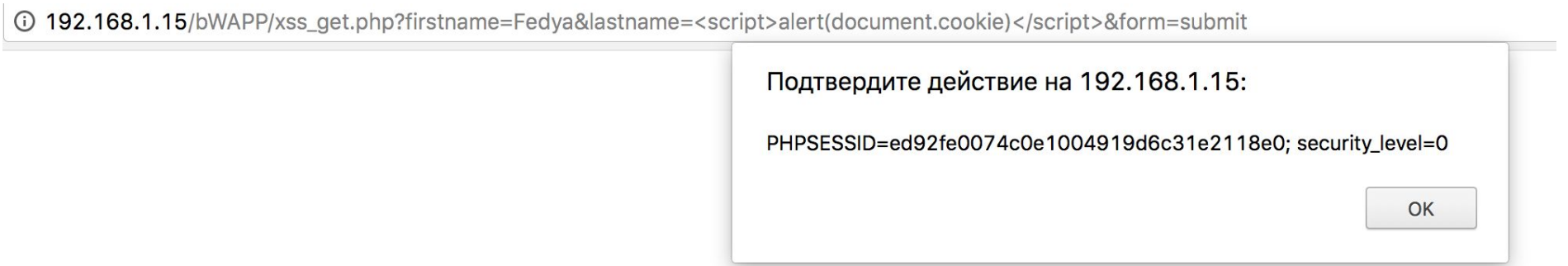
Demo MITM: Intercepter-ng



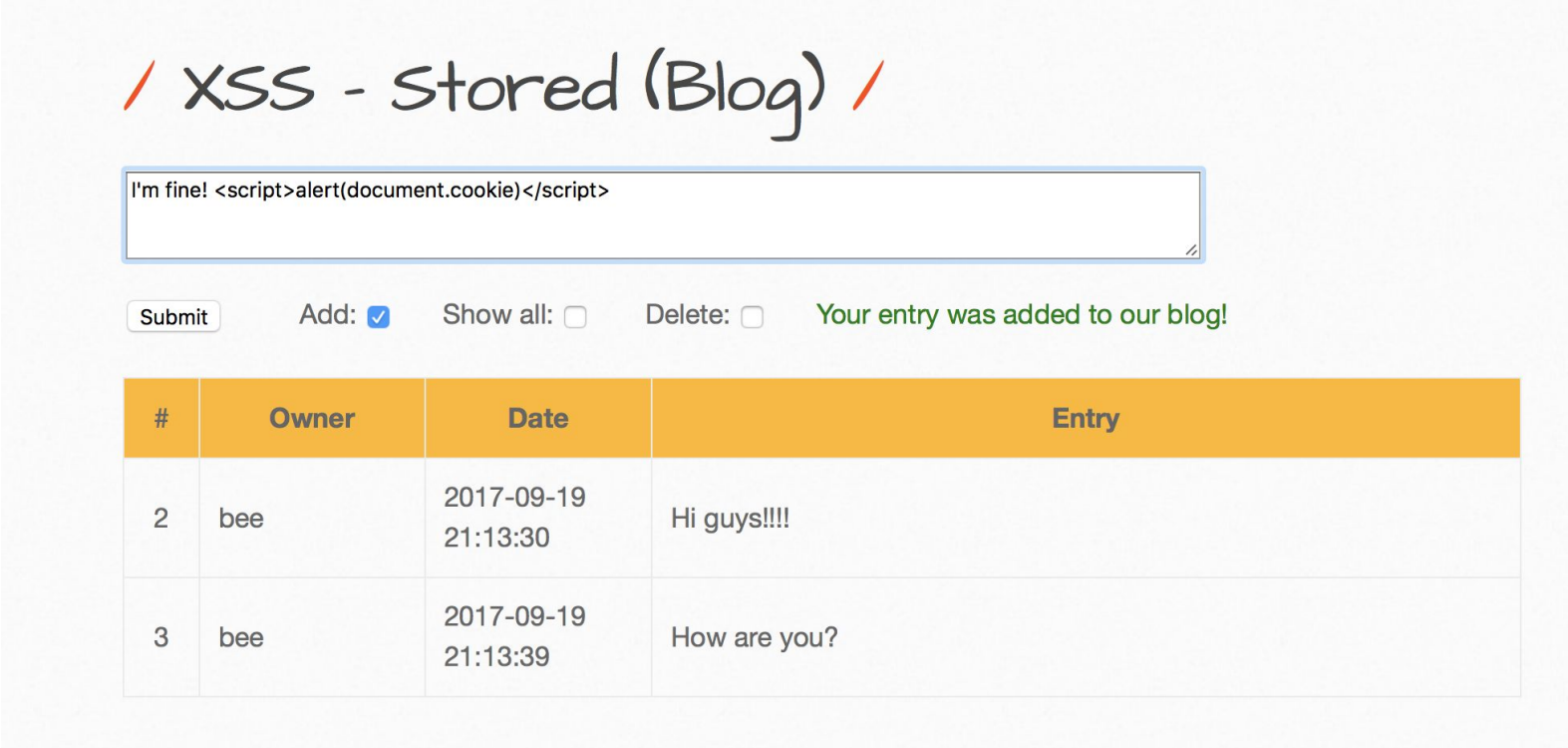


XSS

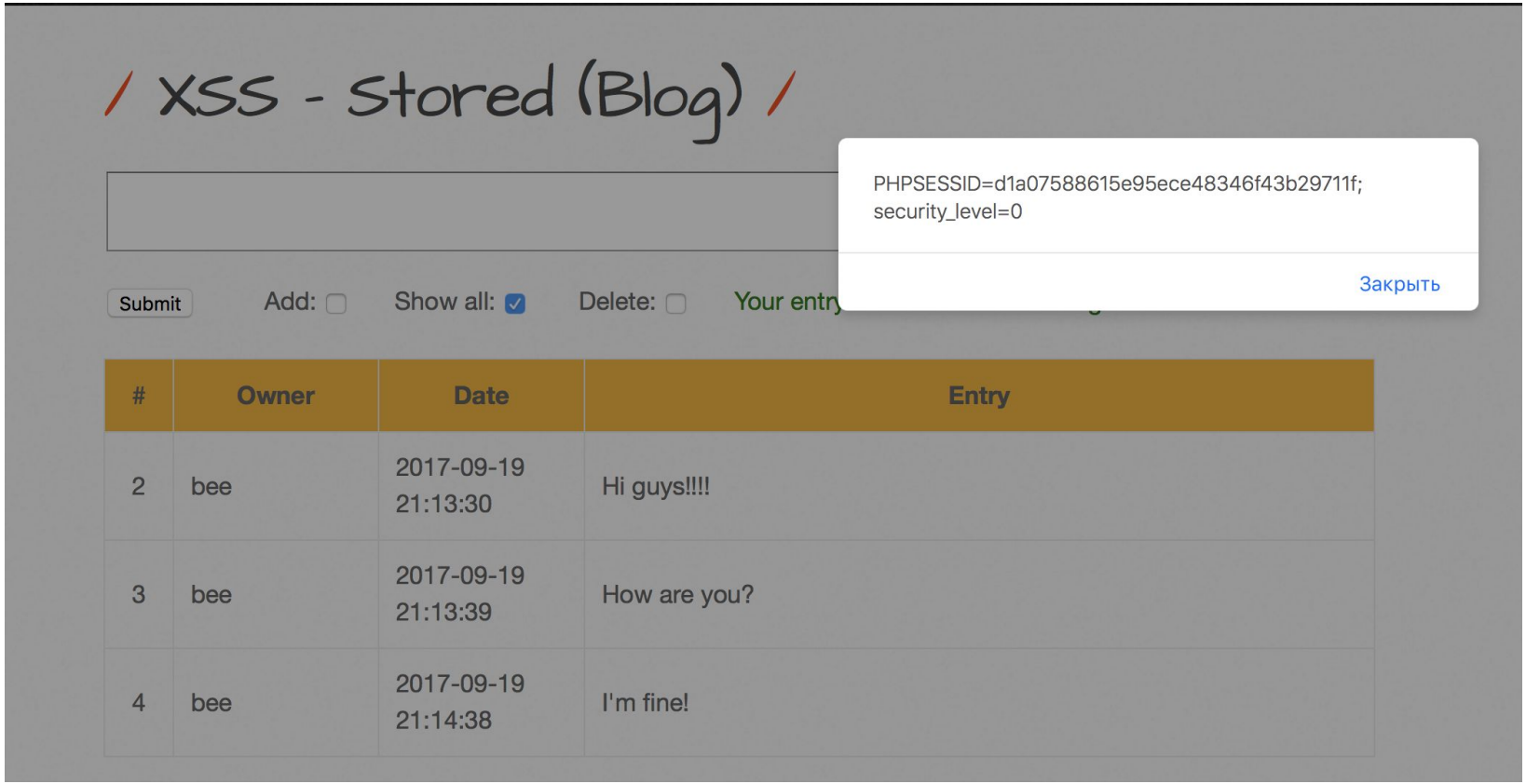
Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites.



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) /
PHPSESSID=d1a07588615e95ece48346f43b29711f;
security_level=0
Закрыть
Submit
Add:
Show all:
Delete:
Your entry
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

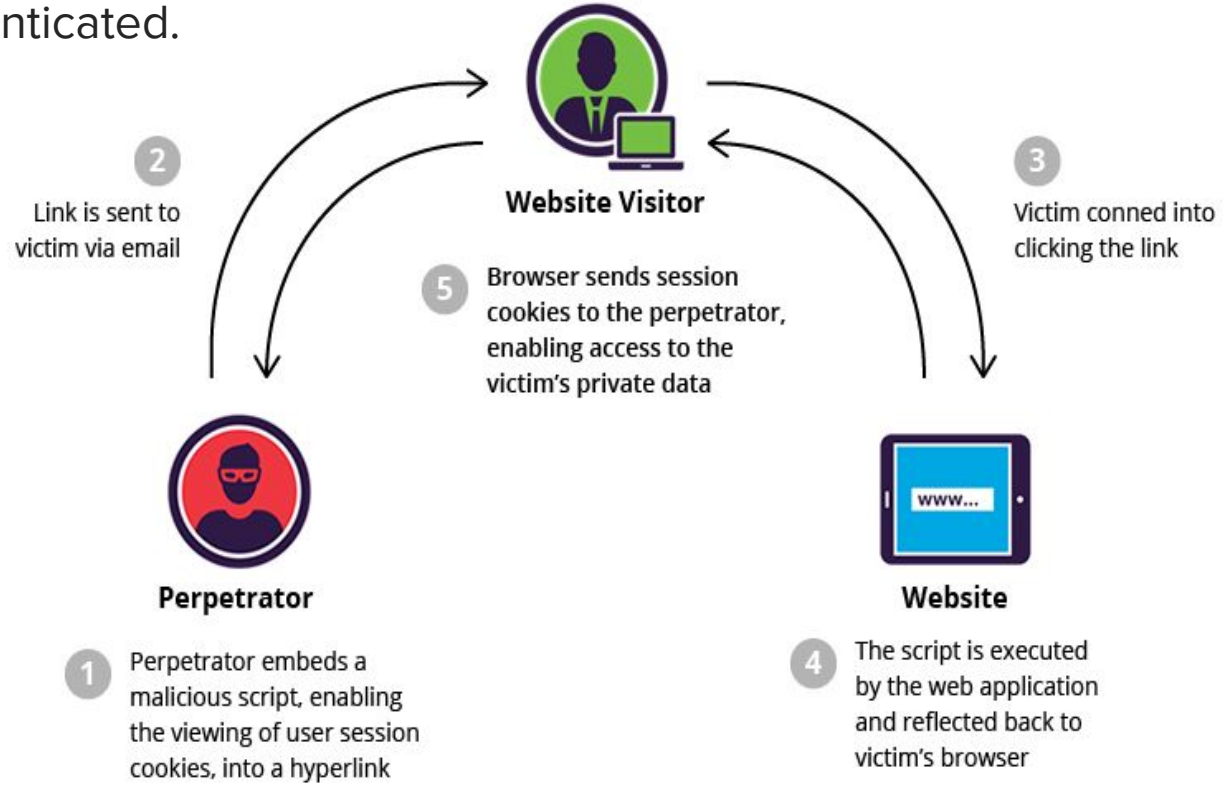
Браузер Chrome обнаружил на этой странице необычный код и заблокировал его, чтобы защитить ваши данные (например, пароли, а также номера телефонов и банковских карт).

Попробуйте открыть главную страницу сайта.

ERR_BLOCKED_BY_XSS_AUDITOR

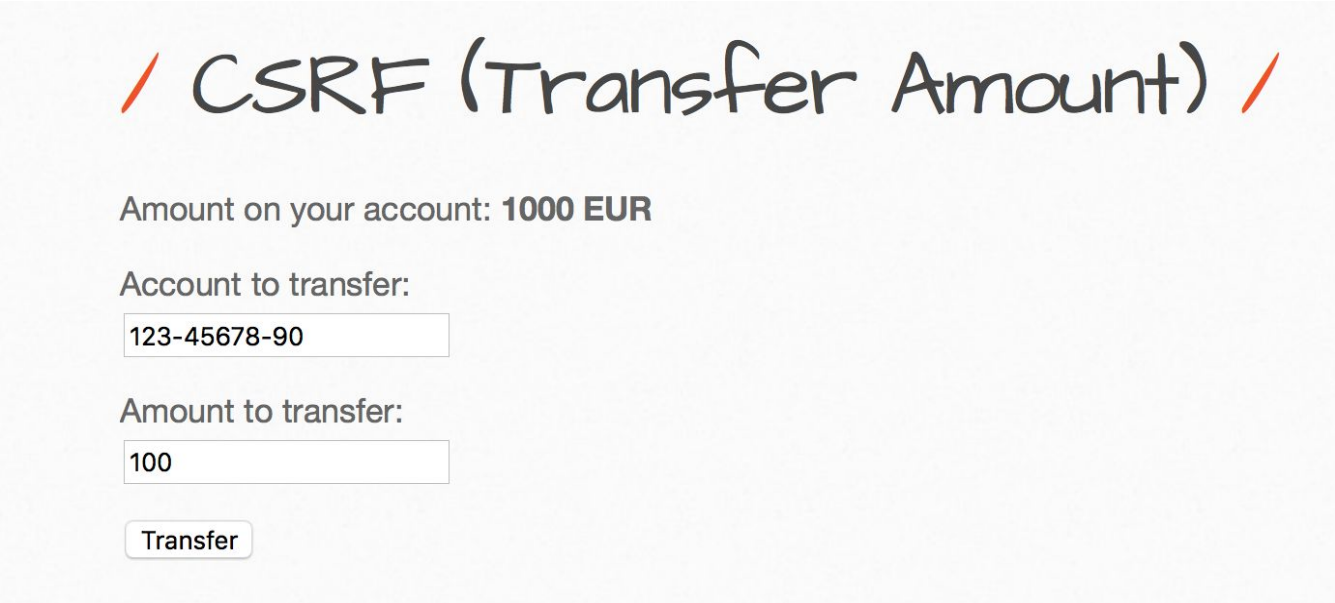
CSRF

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.

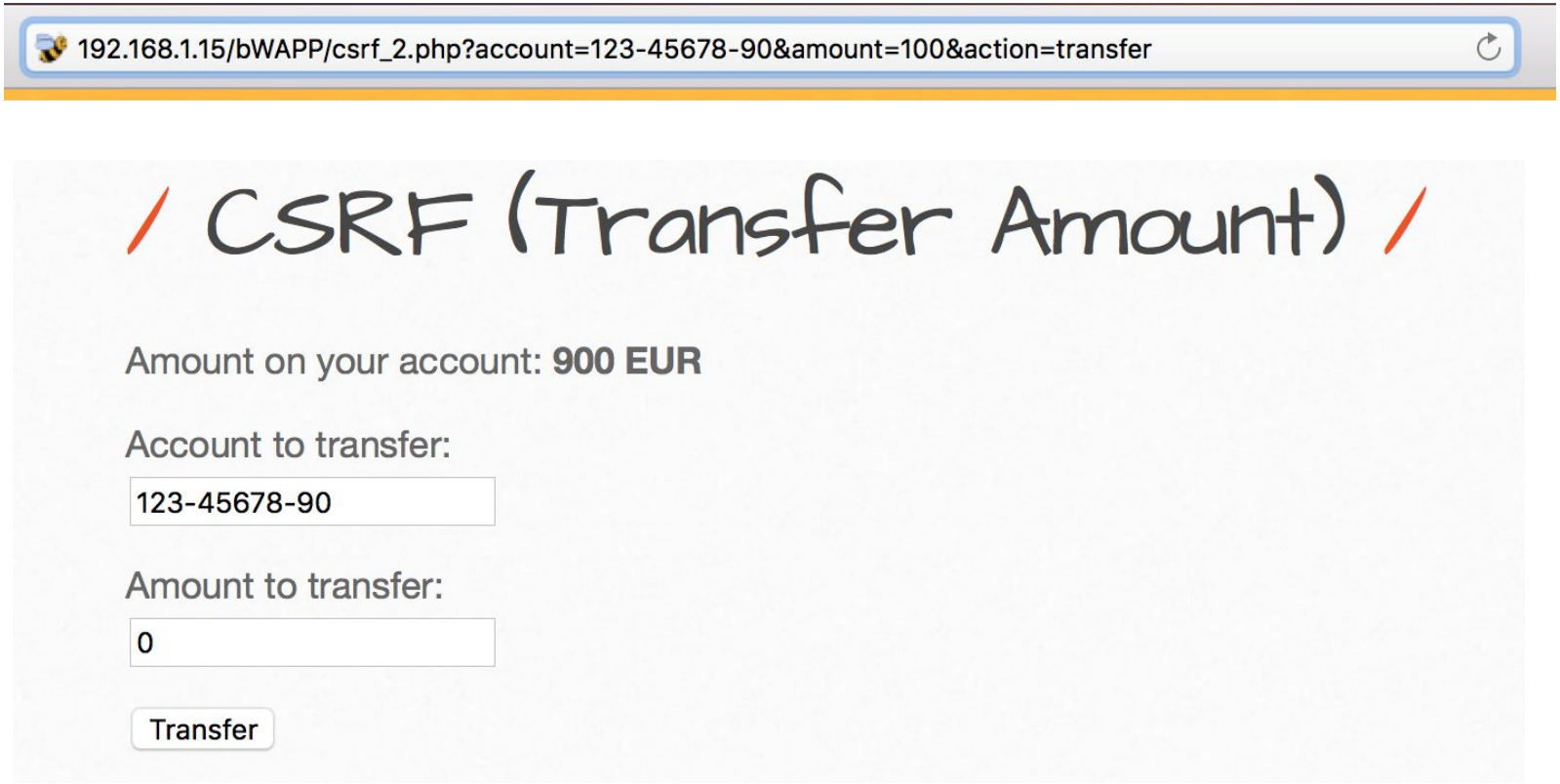


CSRF

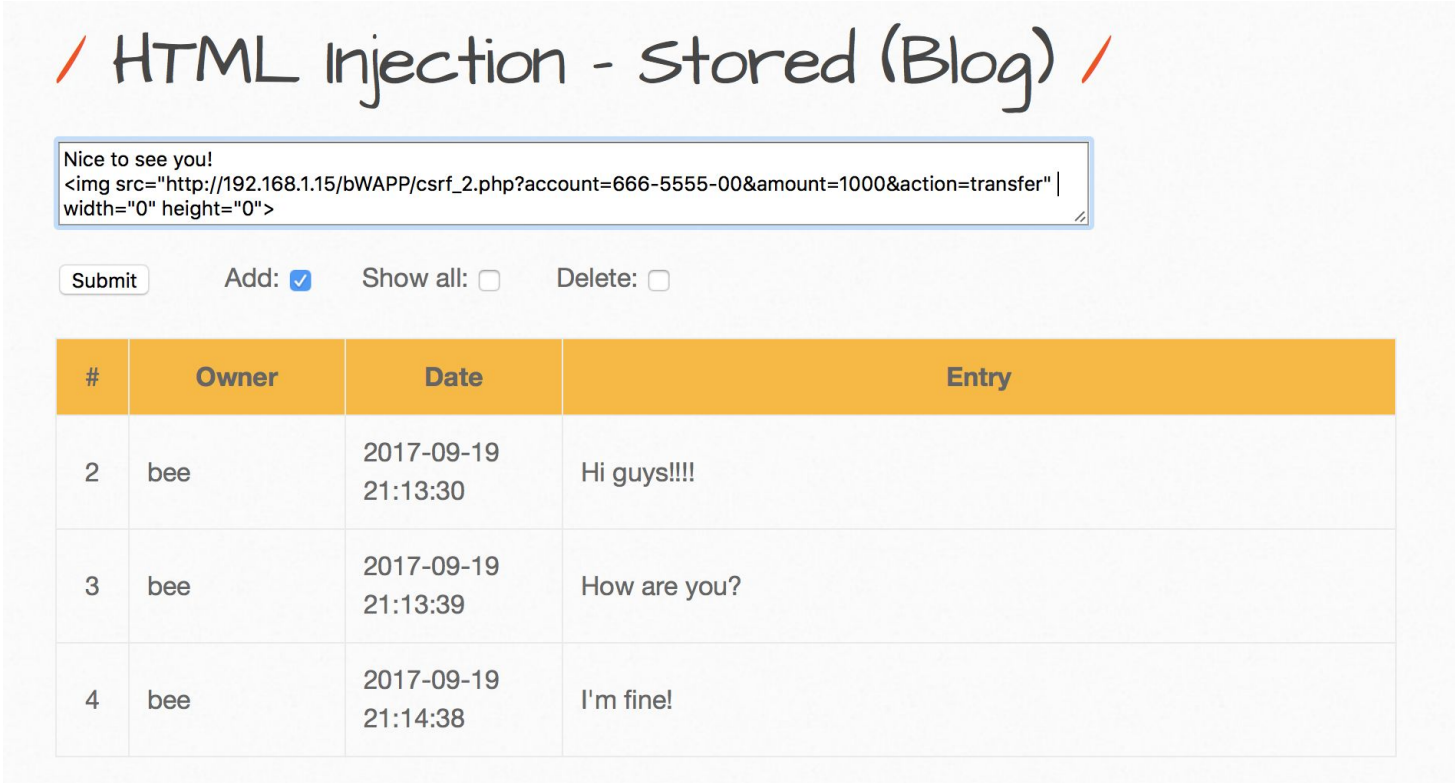
Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated.



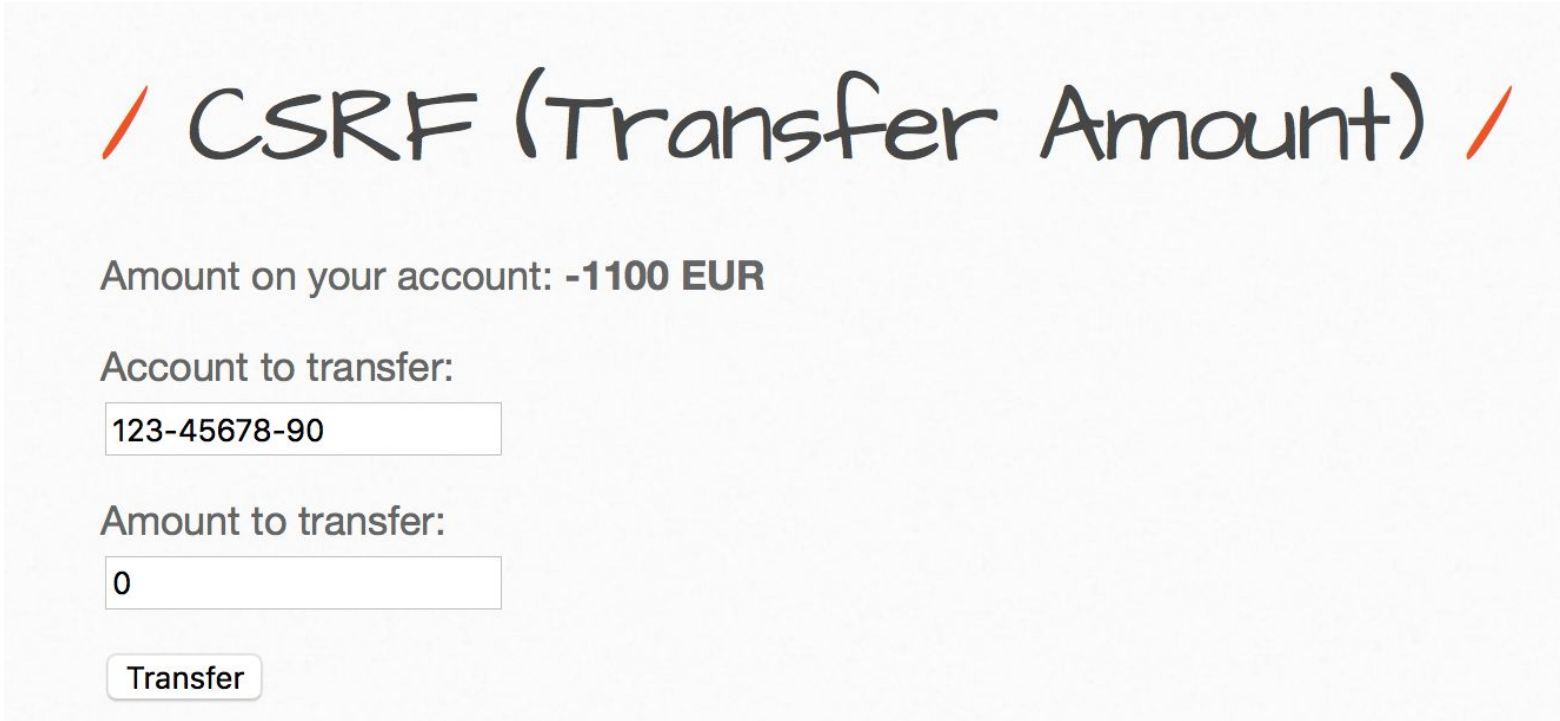
CSRF


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:
123-45678-90
Amount to transfer:
0
Transfer

CSRF

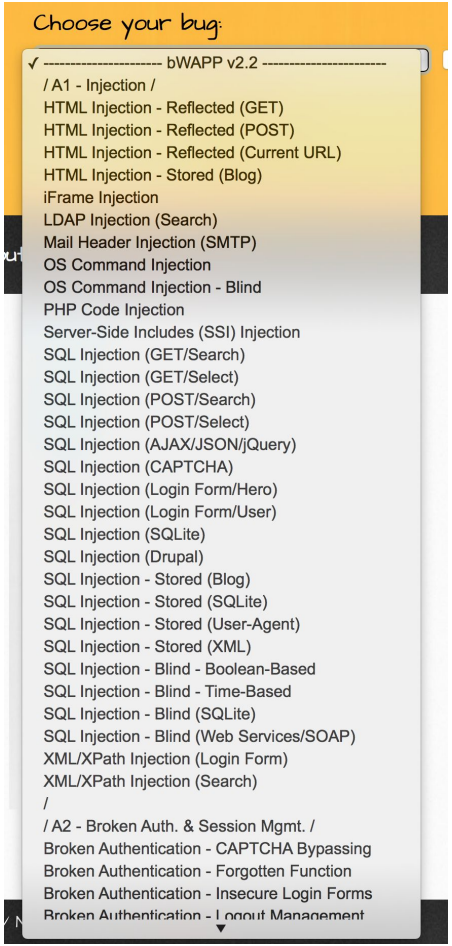

/ HTML Injection - Stored (Blog) /
Nice to see you!
<img src="http://192.168.1.15/bWAPP/csrf_2.php?account=666-5555-00&amount=1000&action=transfer"
width="0" height="0">
Submit
Add:
Show all:
Delete:
Owner Date Entry
2 bee 2017-09-19 21:13:30 Hi guys!!!!
3 bee 2017-09-19 21:13:39 How are you?
4 bee 2017-09-19 21:14:38 I'm fine!

CSRF


/ CSRF (Transfer Amount) /
Amount on your account: -1100 EUR
Account to transfer:
123-45678-90
Amount to transfer:
0
Transfer

How vulnerabilities works ?

http://www.itsecgames.com



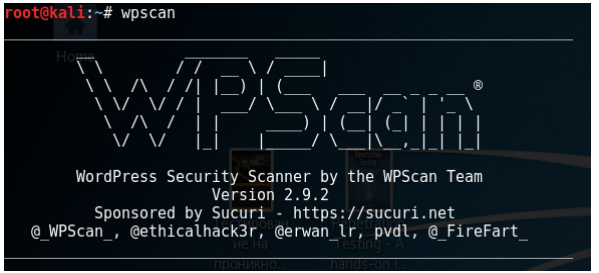
Where i can read about vulnerabilities ?

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:



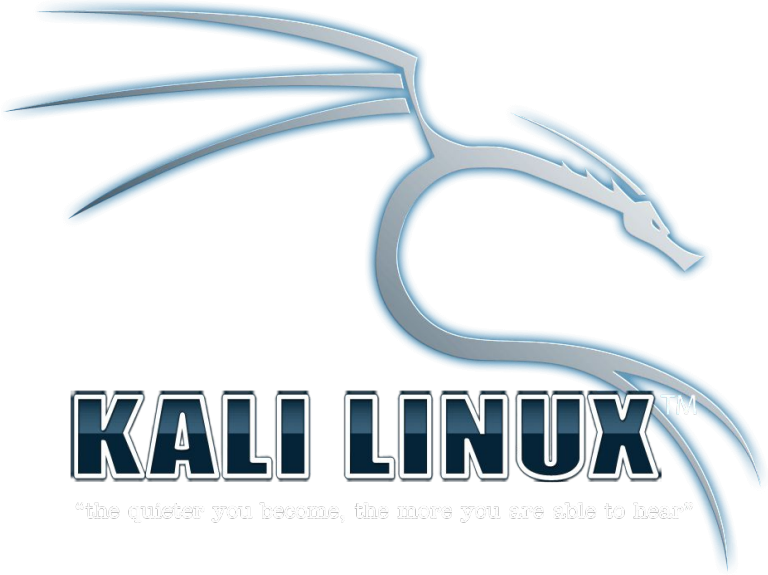
File Edit View Search Terminal Help

```
[!] 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 ?

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.

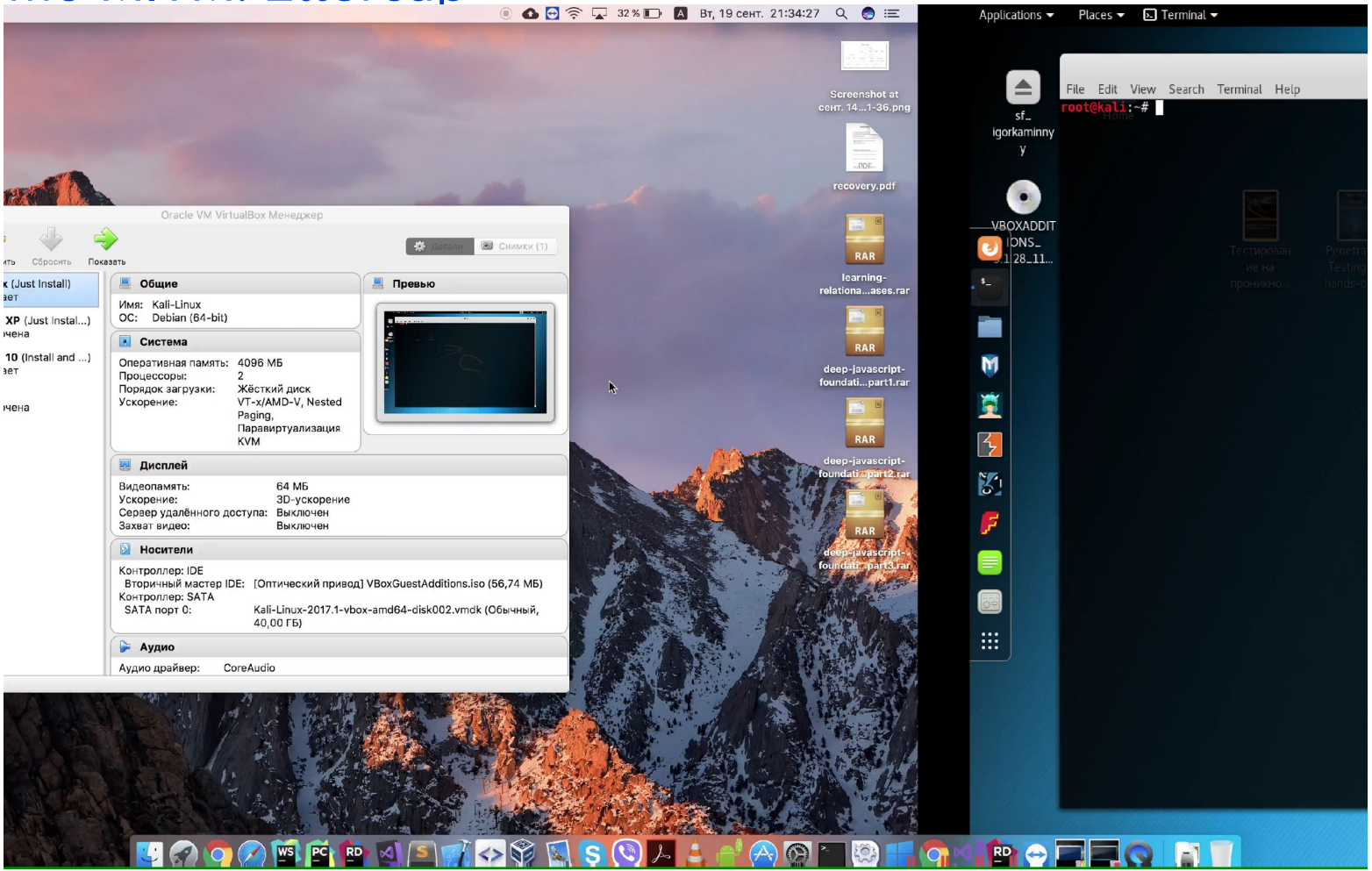
How to get started ?



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/0F3lT)
- 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?