Web программирование

Web Security

Игорь Родионов

Омский Государственный Технический Университет

кафедра Информатики и вычислительной техники

ОмГТУ, 2014.

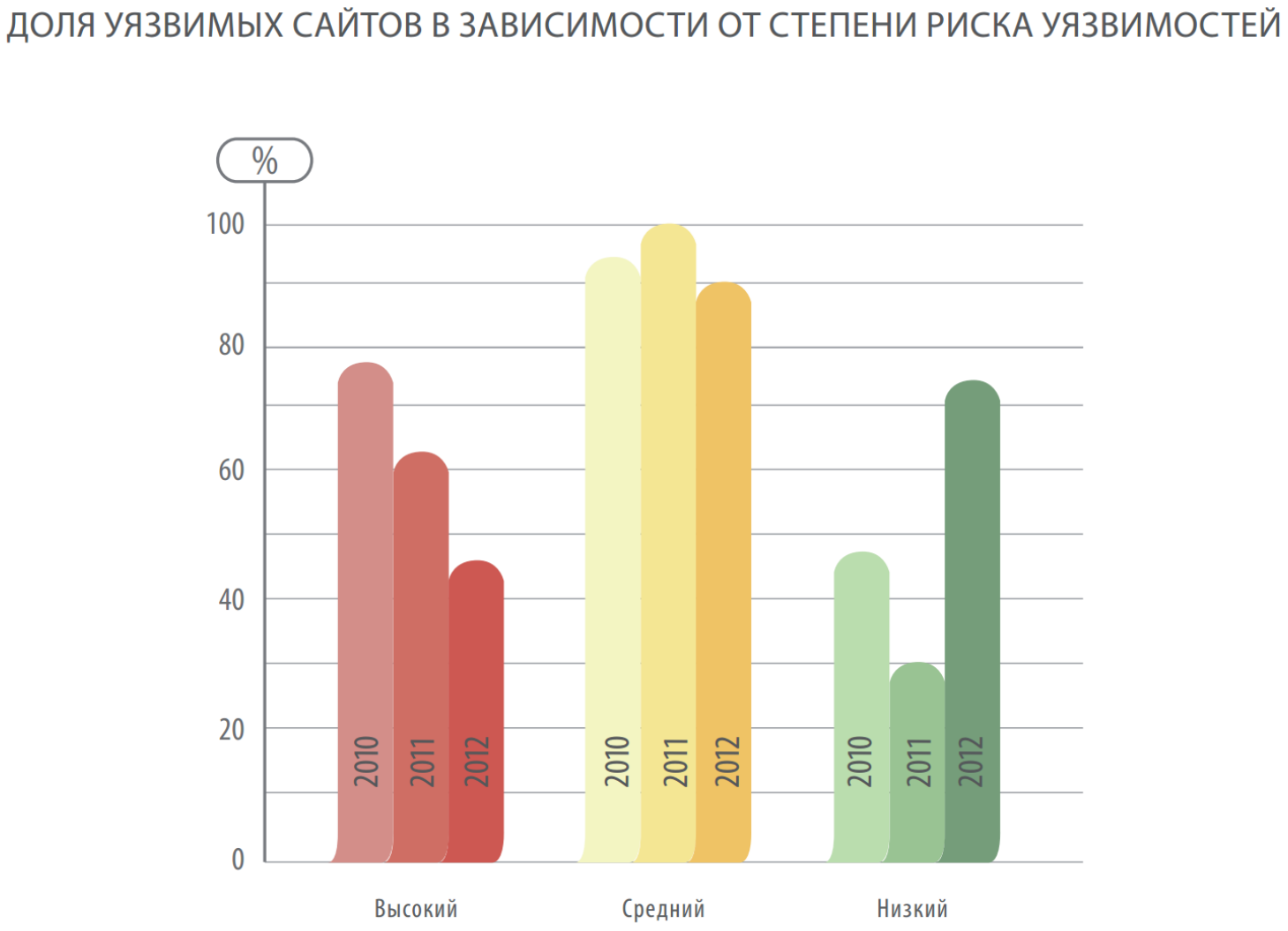
Main Rule

НЕ ДОВЕРЯЙТЕ
ВХОДНЫМ ДАННЫМ

Statistic


НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ УЯЗВИМОСТИ (доля сайтов, %)
Fingerprinting
73%
Cross-Site Scripting
63%
Brute Force
46%
SQL Injection
33%
Cross-Site Request Forgery
31%
Credential/Session Prediction
30%
Server Misconfiguration
30%
Information Leakage
24%
Path Traversal
18%
URL Redirector Abuse
18%

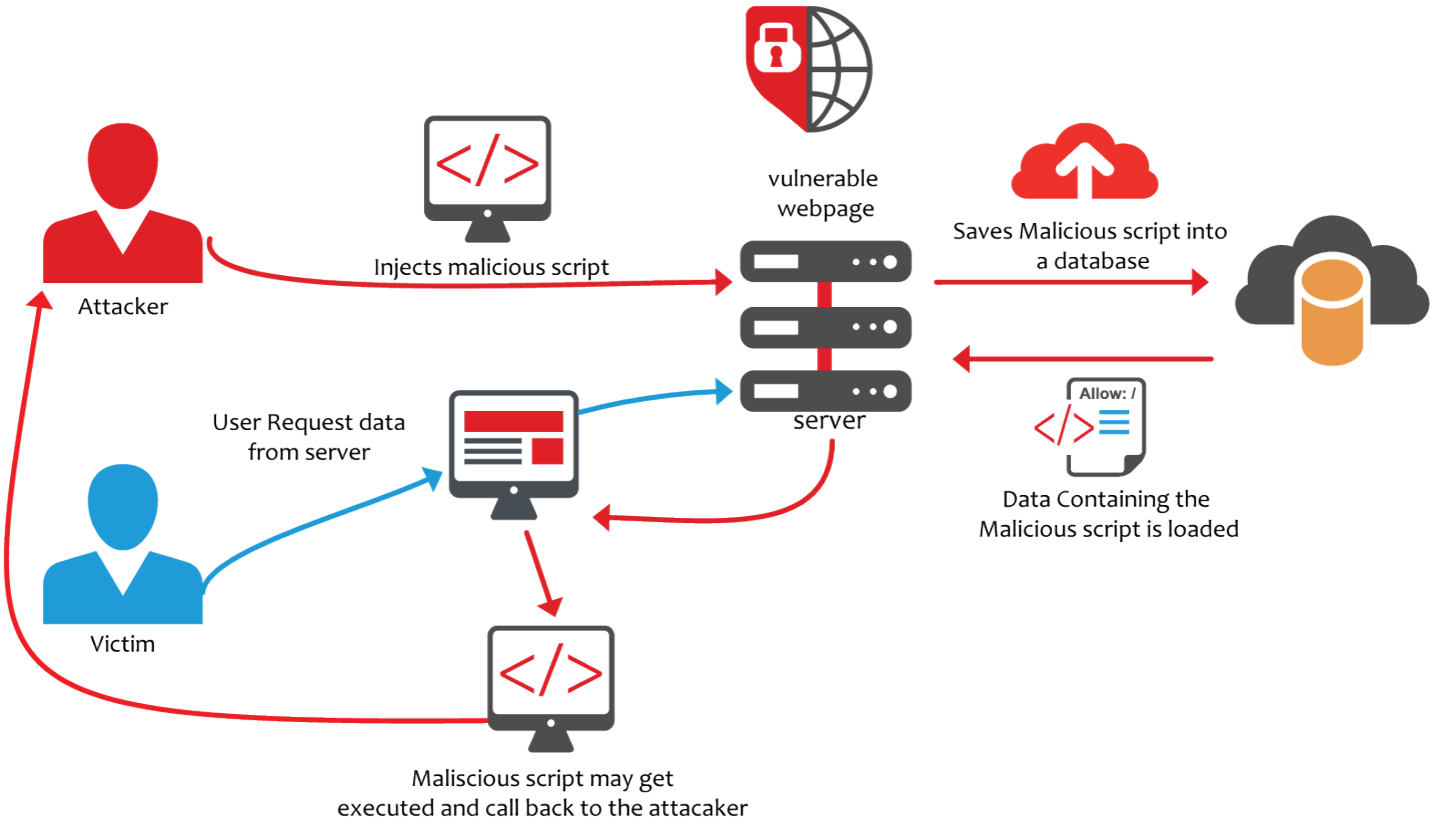
Statistic years



Statistic


НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ УЯЗВИМОСТИ (доля сайтов, %)
Fingerprinting
73%
Cross-Site Scripting
63%
Brute Force
46%
SQL Injection
33%
Cross-Site Request Forgery
31%
Credential/Session Prediction
30%
Server Misconfiguration
30%
Information Leakage
24%
Path Traversal
18%
URL Redirector Abuse
18%

Cross-site Scripting



Questions

Вопросы?

Statistic


НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ УЯЗВИМОСТИ (доля сайтов, %)
Fingerprinting
73%
Cross-Site Scripting
63%
Brute Force
46%
SQL Injection
33%
Cross-Site Request Forgery
31%
Credential/Session Prediction
30%
Server Misconfiguration
30%
Information Leakage
24%
Path Traversal
18%
URL Redirector Abuse
18%

SQL injection

```
1 <?php
2
3 $id = $_REQUEST['id'];
4 $res = mysql_query("SELECT * FROM news WHERE
      id_news = $id");
```

SQL injection

```
1 SELECT * FROM news WHERE id_news = 5
2
3 SELECT * FROM news WHERE id_news = -1 OR 1=1
4
5 SELECT id_news, header, body, author FROM news WHERE
      id_news = -1
6   UNION SELECT 1,username,password,1 FROM admin
7
8 SELECT * FROM news WHERE id_news = 12;
9 INSERT INTO admin (username, password) VALUES ('
      HaCkEr', 'foo');
```

SQL injection

SQL injection

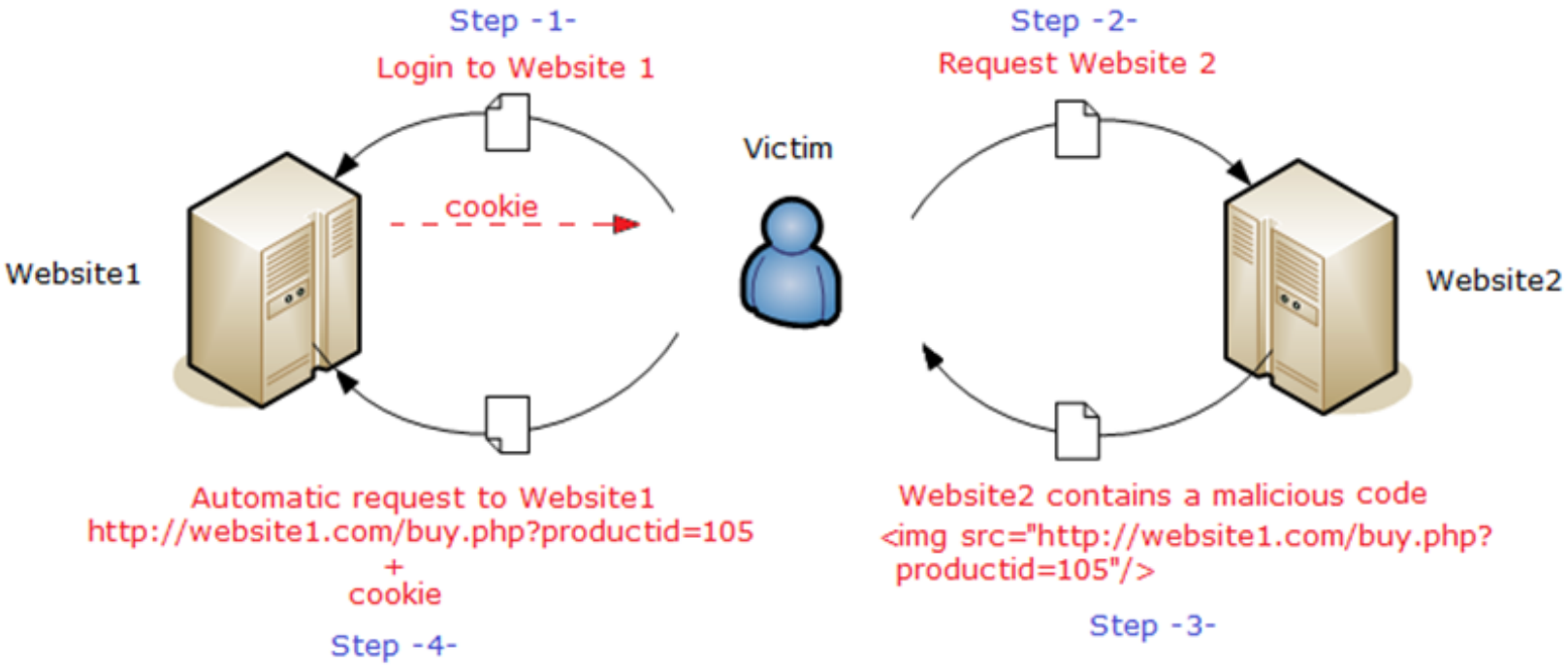
Questions

Вопросы?

Statistic


НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ УЯЗВИМОСТИ (доля сайтов, %)
Fingerprinting
73%
Cross-Site Scripting
63%
Brute Force
46%
SQL Injection
33%
Cross-Site Request Forgery
31%
Credential/Session Prediction
30%
Server Misconfiguration
30%
Information Leakage
24%
Path Traversal
18%
URL Redirector Abuse
18%

Cross Site Request Forgery



Questions

Вопросы?

References

Статистика уязвимостей
веб-приложений 2012
http://goo.gl/Ng258w

Статистика уязвимостей
веб-приложений за 2010-2011 годы
http://goo.gl/zGxlWX

Additional

www.ptsecurity.ru

www.owasp.org