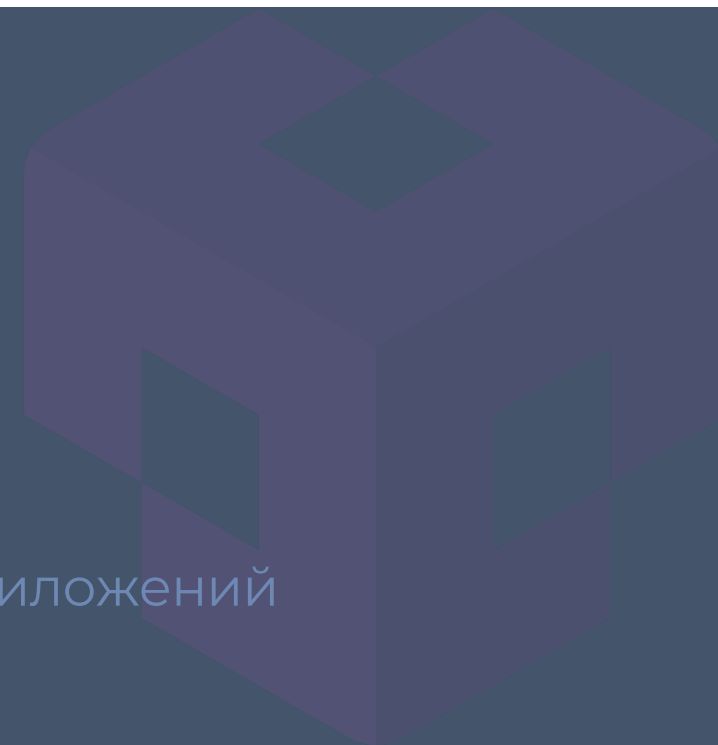


SolidPoint DAST

Интеллектуальный сканер безопасности веб приложений
и сервисов



Валерий Куваев
Менеджер по продукту
Valeriy.kuvaev@solidlab.ru



Dynamic Analysis
for Security Testing

Основные задачи

- Обнаружение максимальной поверхности атаки
- Обнаружение критических уязвимостей в первую очередь
- Масштабирование и поддержка мультитенантности
- Интеграция в сценарии CI\CD и возможность интерактивного запуска
- Поддержка специфических технологий Заказчиков

Обнаружение поверхности атаки

- Интеллектуальный инструмент для анализа защищенности веб-приложений методами статико-динамического анализа
- Сканирование сети, выявление уязвимостей в инфраструктуре доставки приложений
- Максимальная эффективность при поиске точек ввода данных в приложение (Data Entry Points)
- Уникальные технологии статико-динамического анализа JavaScript кода¹

¹ Статья: <http://journals.tsu.ru/engine/download.php?id=223281&area=files>

Выступление: <https://www.youtube.com/watch?v=vG0EzOr8lpE>

Обнаружение поверхности атаки

Применяемые методы

- Static & Dynamic Crawling
- Dirbusting
- Статико-динамический анализ клиентского JS кода
- OpenAPI import
- FAST (интеграция с SolidWall WAF)
- Импорт HAR*
- Сканирование IP/Диапазона для выявления

* В разработке

Сканеры безопасности

Критические риски в первую очередь



Insecure Deserialization

Reflected XSS

XXE

NoSQLi

SQLi

Path Injection*

HTTP Smuggling

File Upload

Prototype Pollution

DOM Based XSS

Пассивный сигнатурный анализ

Активный сигнатурный анализ

Перебор паролей

*В разработке

Изменение цели

✓

Информация о цели

2

Аутентификация

3

Предпросмотр

Аутентификация

Включить аутентификацию

Данные аутентификации

+

Данные аутентификации не добавлены

Cookie

Заголовок запроса

HTTP Basic Auth

POST /api/targets create new target

create new target. Use "Content-Type: multipart/form-data" for data with files. Allowed r

Parameters

Name	Description
createTargetData required	Target Create Data
object	Example Value Model

```
fuchsiactl scan [flags]

Flags:
  --authchecking-config string    Path to file with a
  --cookie cookie                Extra HTTP cookie (
me of the scan). Example: "name=value; name2=value2"
  --dirbusting                   Enable dirbusting v
  --domain-list domainList       Comma-separated lis
r domain-scope == Same or Subdomain) (default [])
  --domain-scope domain-scope    Domain filtering m
dlevel/second-level) (default any)
  --exposeAddress URL            URL to scan applica
  --file extraFileList           Pass additional fil
: ${name}=${contents} or --file=${module}:${name}@${path})
  --header header                Extra HTTP header (
me of the scan). Example: "X-Token: foobar"
  -h, --help                     help for scan
  --max-rps float                Maximum RPS (unlimi
  --modules string,...           List of modules to
et)
  --password string              Password for HTTP b
```

```
{
  "appAuth": {
    "certificates": [
      {
        "certificate": "string",
        "key": "string"
      }
    ],
    "cookies": [
      {
        "hostname": "string",
        "name": "string",
        "path": "string",
        "port": "string",
        "value": "string"
      }
    ]
  }
}
```

Parameter content type
application/json

Аутентификация

Используется MITM Proxy

Технологии:

HTTP Basic Authentication
Header
Cookies
X.509

Активный рефреш сессий*

Использование сценария автоматической аутентификации*

*В разработке

Развертывание и масштабирование

- Apt пакеты (Ubuntu\Debian)
- Docker контейнеры и Docker-compose.yml
- Kubernetes*

*В разработке



Vulnerabilities 1234

Brian Holland
nickey_mouse@gmail.com

Dashboard

Scans

Scheduler

Targets

Target groups

Organizations

Users

Reports

[Home](#) >
 [Scans](#) >
 [Scan 1234](#) >
 Vulnerabilities 1234

RETEST MARK AS

Found: 8 vulnerabilities
 1
1
2
2
0

	Vulnerability	URL	Parameter	Status	Confidence, %	
☐	■ Joomla! Core 3.x.x Cross-Sit...	https://www.rbc.ru/...	task	Open	90	⋮
☐	■ Joomla! Core 3.x.x Cross-Sit...	https://www.rbc.ru/...	<empty>	False Positive	90	⋮
☐	■ Joomla! Core 3.x.x Cross-Sit...	https://www.rbc.ru/...	task	Fixed	90	⋮
☐	■ Joomla! Core 3.x.x Cross-Sit...	https://www.rbc.ru/...	task	Open	Open	✓ Mark as >
☐	■ Joomla! Core 3.x.x Cross-Sit...	https://www.rbc.ru/...	task	False Positiv	Fixed	Retest
☐	■ Joomla! Core 3.x.x Cross-Sit...	https://www.rbc.ru/...	task	False Positiv	Ignored	
☐	■ Joomla! Core 3.x.x Cross-Sit...	https://www.rbc.ru/...	task	False Positiv	False Positive	90 ⋮
☐	■ Joomla! Core 3.x.x Cross-Sit...	https://www.rbc.ru/...	task	Fixed	90	⋮
☐	■ Joomla! Core 3.x.x Cross-Sit...	https://www.rbc.ru/...	task	Fixed	90	⋮

What's new?

Knowledge base

Contact us



Демо



Q&A