セクコン株式会社 御中

セキュリティ診断報告書

2015年8月26日

TeamC

おことわり

- SandBag
  - アプリ～サーバの通信に着目
  - 通信内容を変化させた時の
    - サーバの挙動
    - クライアントの挙動
  - サーバの堅牢さ

自己紹介

- まつもとじゅん
  - SECCON 2013 決勝戦 14位
  - SECCON 2014 オンライン予選 51位

目次

- 診断結果総評
- 脆弱性の評価レベル
- 診断結果概要
- 診断結果詳細
- 検査ツール・演習環境

診断結果総評

- SandBag
  - 通信部分とサーバに複数の重大な脆弱性
  - 早急な修正を！

脆弱性の評価レベル

Level		内容
3	重大	サーバや他プレイヤーへの影響
2	限定	自環境への影響
1	軽微	不必要な情報開示・サービス稼働

診断結果概要：アプリケーション診断

No.	概要	Level
A1	SQLインジェクションの脆弱性	3
A2	送信パラメータの改ざん	3
A3	受信パラメータのチェック不足	2

診断結果概要：ネットワーク診断

No.	概要	Level
N1	脆弱性が存在するApache(2.2.15)	3
N2	脆弱性が存在するPHP(5.3.3)	3
N3	HTTPヘッダによるバージョン表示	1
N4	推奨しないHTTPメソッドの許可	1
N5	PHP Creditsの表示	1

A1. SQLインジェクションの脆弱性 (Lv.3)

- 発生箇所
  - プレイ後のスコア登録
  - POST http://api.sandbag2015.net/score/ranking/
- 原因
  - サーバが受信したスコア情報を、データベースに登録する際の処理に不備がある
- 影響
  - データベース内容の漏洩、改ざんが可能

SQL

- データベースを操作する**SQLコマンド**と**パラメータ**からなる問い合わせ言語
- 予め用意したSQLコマンドと**利用者からの入力値をパラメータ**としてSQL文を組み立て、データベースサーバで実行

SQLの基礎知識1－1

IPA

- SQLの基本形
  - 特定のテーブルから情報を取り出す場合

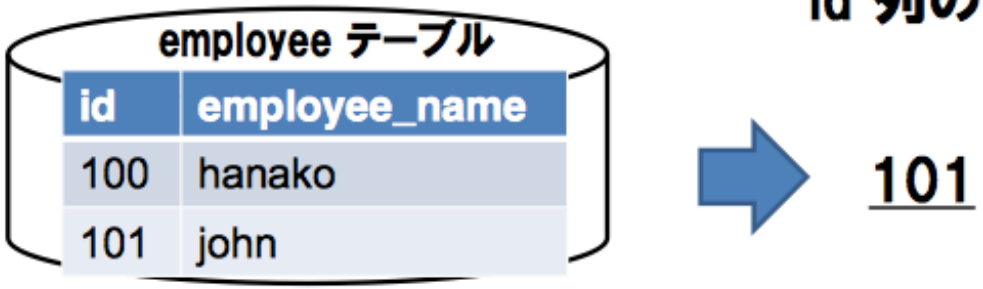
```
SELECT [A] FROM [B] WHERE [C]
```

[B]（テーブル）から［C］の条件で［A］（列の値）を取り出す

例

```
SELECT id FROM employee WHERE employee_name = 'john'
```

employee テーブルから
　employee_name = ‘john‘ となる条件で
　　id 列の値を取り出す



Copyright © 2015 独立行政法人情報処理推進機構

SQLインジェクション攻撃

- SQL文の組み立て方法に問題があるプログラムの**不備を突き**、**入力パラメータに混入したSQLコマンドを実行**
- 想定しないSQL文が実行され**データベースを不正に操作**（認証突破、情報漏洩、改ざん、バックドアのアップロードなど）

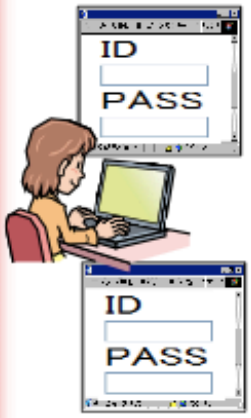
SQLを使った認証判定の例（通常時）

- ログインページでの認証判定では、SQLが使われることが多い。

認証判定SQL: `SELECT * FROM user WHERE id='ID' AND pass='PASS'`

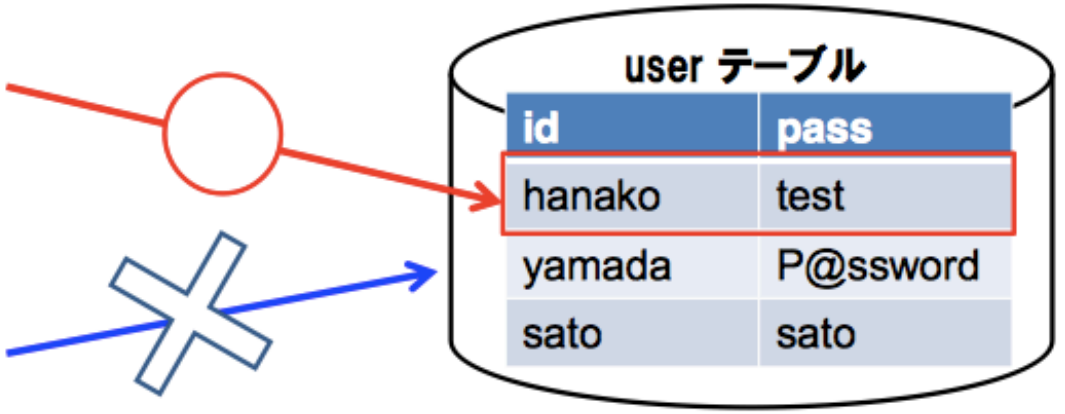
user テーブルで id が ID で pass が PASS な行が1つ以上あれば認証可、0なら認証不可

例）



id=hanako
pass=test

id=hanako
pass=123



Copyright © 2015 独立行政法人情報処理推進機構

SQLを使った認証判定の例(攻撃時)

- 攻撃者は‘(シングルクォート)と-- (コメント)を使って攻撃

認証判定SQL: `SELECT * FROM user WHERE id= ' ID ' AND pass= ' PASS '`

id=hanako' --

pass=123

コメント

`SELECT * FROM user WHERE id= ' hanako' -- ' AND pass=' 123'`

user テーブルで id が hanako ~~で pass が 123~~ な行が

1つ以上あれば認証可、0なら認証不可

user テーブル

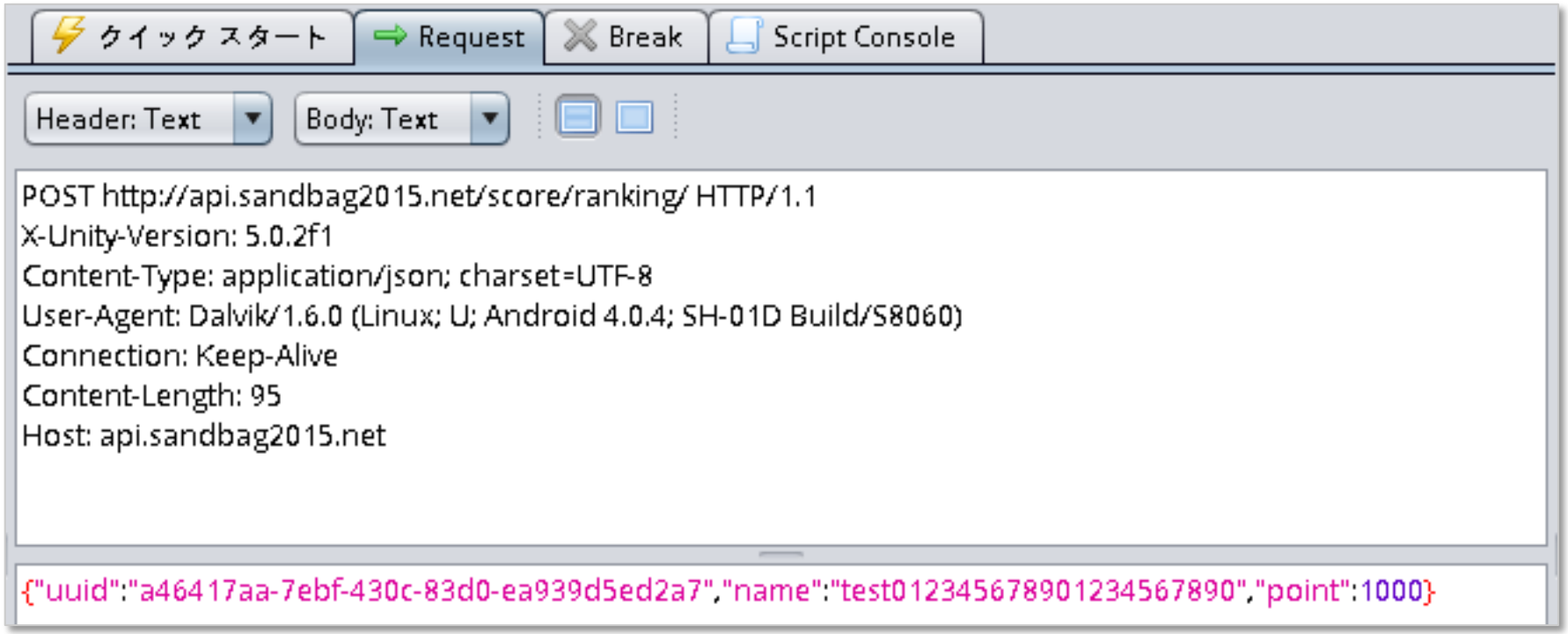
id	pass
hanako	test
yamada	P@ssword

パスワードを知らなくてもログインされてしまう

Copyright © 2015 独立行政法人情報処理推進機構

A1. SQLインジェクションの脆弱性 (Lv.3)

- 検査ツール (OWASP ZAP) でのキャプチャ例



A1. SQLインジェクションの脆弱性 (Lv.3)

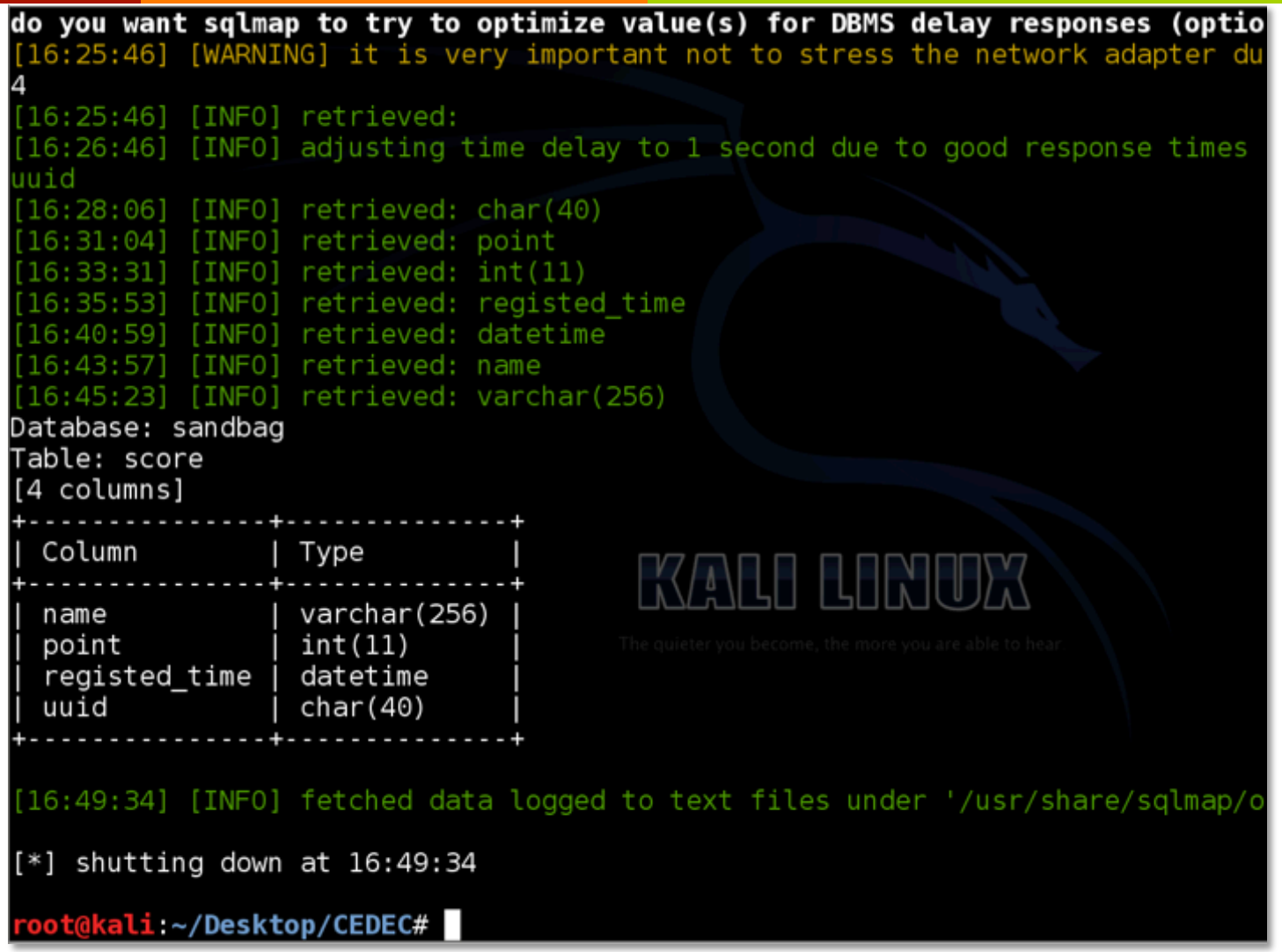
- 検査ツール(sqlmap)での確認事例
  - 検査パラメータ送信時のサーバの挙動より、SQLインジェクションを検知
    - {"uuid":"a46417aa-7ebf-430c-83d0-ea939d5ed2a7","name":"test0123456789012345678 90","point":"1000**; SELECT SLEEP(5)--** "}
    - {"uuid":"a46417aa-7ebf-430c-83d0-ea939d5ed2a7","name":"test0123456789012345678 90","point":"1000 **AND SLEEP(5)**”}

A1. SQLインジェクションの脆弱性 (Lv.3)

- データベースサーバの内部情報を取得

Database	sandbag
Table	score
Column	name, point, registed_time, uuid （値も取得可能）

A1. SQLインジェクションの脆弱性 (Lv.3)



A1. SQLインジェクションの脆弱性 (Lv.3)

- 対策
  - SQL文を作成する際に「SQLコマンド」と「利用者からの入力値」を**単純に連結しない**
  - 安全な方法でSQL文を作成する
    - プレースホルダ、バインド

A1. SQLインジェクションの脆弱性 (Lv.3)

- **プレースホルダ**
  - SQL文を構成する「SQLコマンド」と「パラメータが入る箇所」を**分けて定義**
- **バインド**
  - 「パラメータが入る箇所」に「利用者からの入力値」を**安全に埋め込む**
- 混入された「SQLコマンド」は実行されない

IPA 資料

- 「安全なウェブサイトの作り方」
- 「安全なSQLの呼び出し方」

https://www.ipa.go.jp/security/vuln/websecurity.html

A2. 送信パラメータの改ざん (Lv.3)

- 発生箇所
  - プレイ後のスコア登録
  - POST http://api.sandbag2015.net/score/ranking/
- 原因
  - スコア登録時のPOST通信が平文
  - 改ざんチェックの仕組みが無い

A2. 送信パラメータの改ざん (Lv.3)

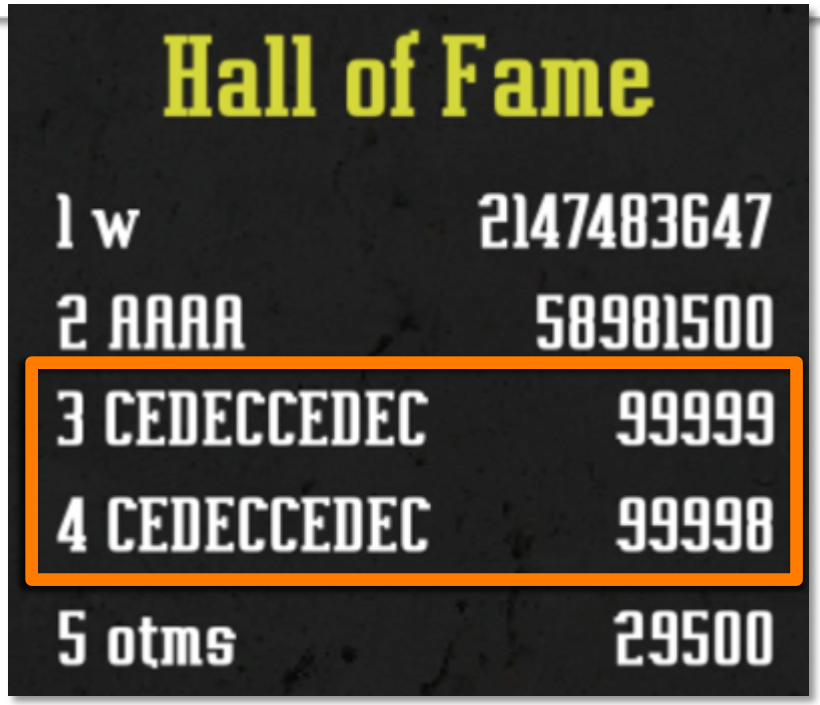
- 影響
  - 自分のスコアを水増しして登録
  - ランキング荒らし（適当な名前、スコアで登録）
- 確認手順
  - Proxyツールなどで、サーバに送信するパラメータを書き換える

A2. 送信パラメータの改ざん (Lv.3)

- 再現例
  - スコアの改ざん
    - {"uuid":"a46417aa-7ebf-430c-83d0-ea939d5ed2a7","name":"test0123","point":"1000**0000**"}
  - 未登録のuuidで任意のname, pointを登録
    - {"uuid":"a46417aa-7ebf-430c-83d0-ea939d5ed2a**8**","name":”**CEDECCEDEC**","point":”**99999**”}

A2. 送信パラメータの改ざん (Lv.3)


```
{"uuid":"a46417aa-7ebf-430c-83d0-ea939d5ed2a8","name":"CEDECCEDEC",
"point":99999}
{"uuid":"a46417aa-7ebf-430c-83d0-ea939d5ed2a9","name":"CEDECCEDEC",
"point":99998}
```

A2. 送信パラメータの改ざん (Lv.3)

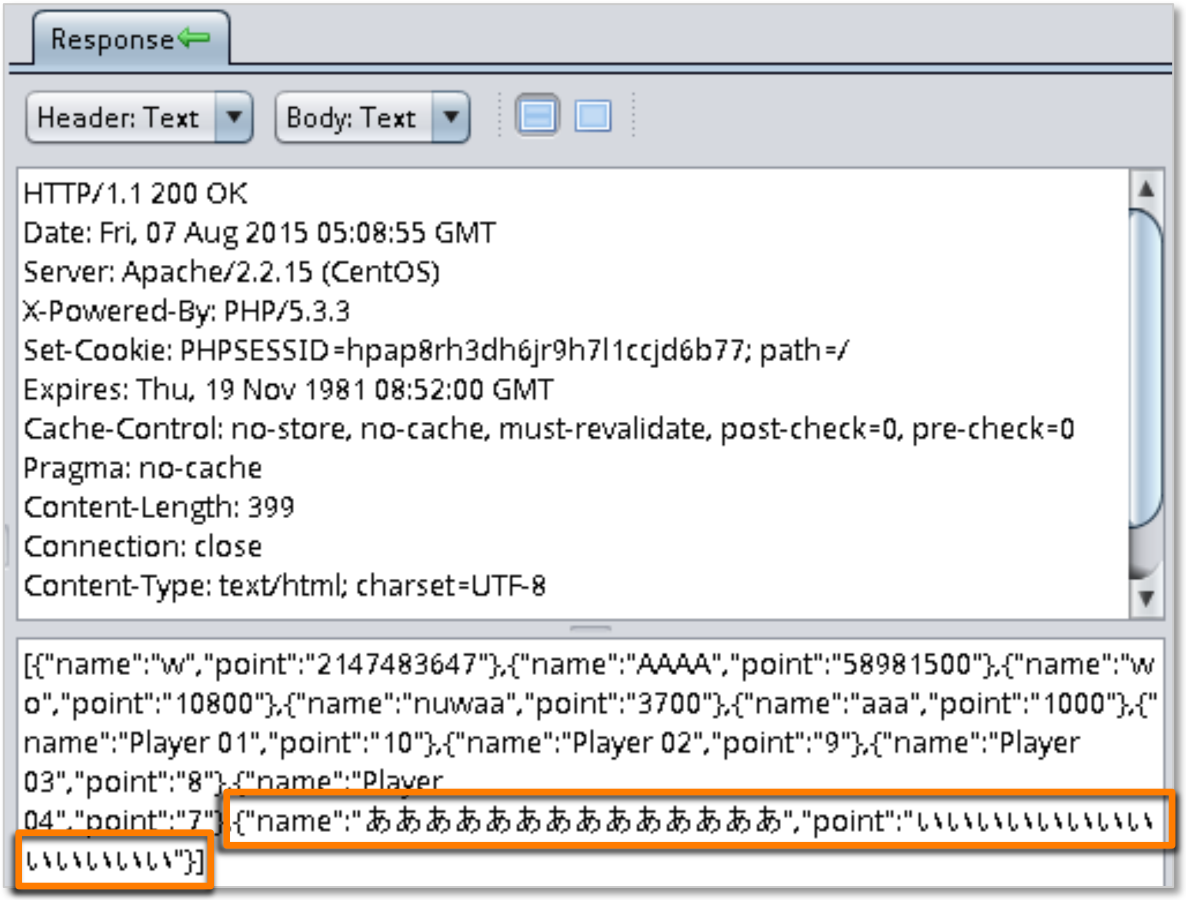
- 対策
  - HTTPSで通信を暗号化
  - 重要なパラメータに別途の暗号化や改ざん検出策を実装

A3. 受信パラメータのチェック不十分 (Lv.2)

- 発生箇所
  - ランキングデータを取得しアプリで表示する部分
  - GET http://api.sandbag2015.net/score/ranking/
- 原因
  - サーバから得たパラメータをそのまま表示

A3. 受信パラメータのチェック不十分 (Lv.2)

- 検査ツール (OWASP ZAP) での改ざん例



A3. 受信パラメータのチェック不十分 (Lv.2)

- 対策
  - HTTPSで通信を暗号化
  - 重要なパラメータに別途の暗号化や改ざん検出策を実装
  - アプリ側で受信パラメータの文字種や桁数などを確認

診断結果概要：ネットワーク診断

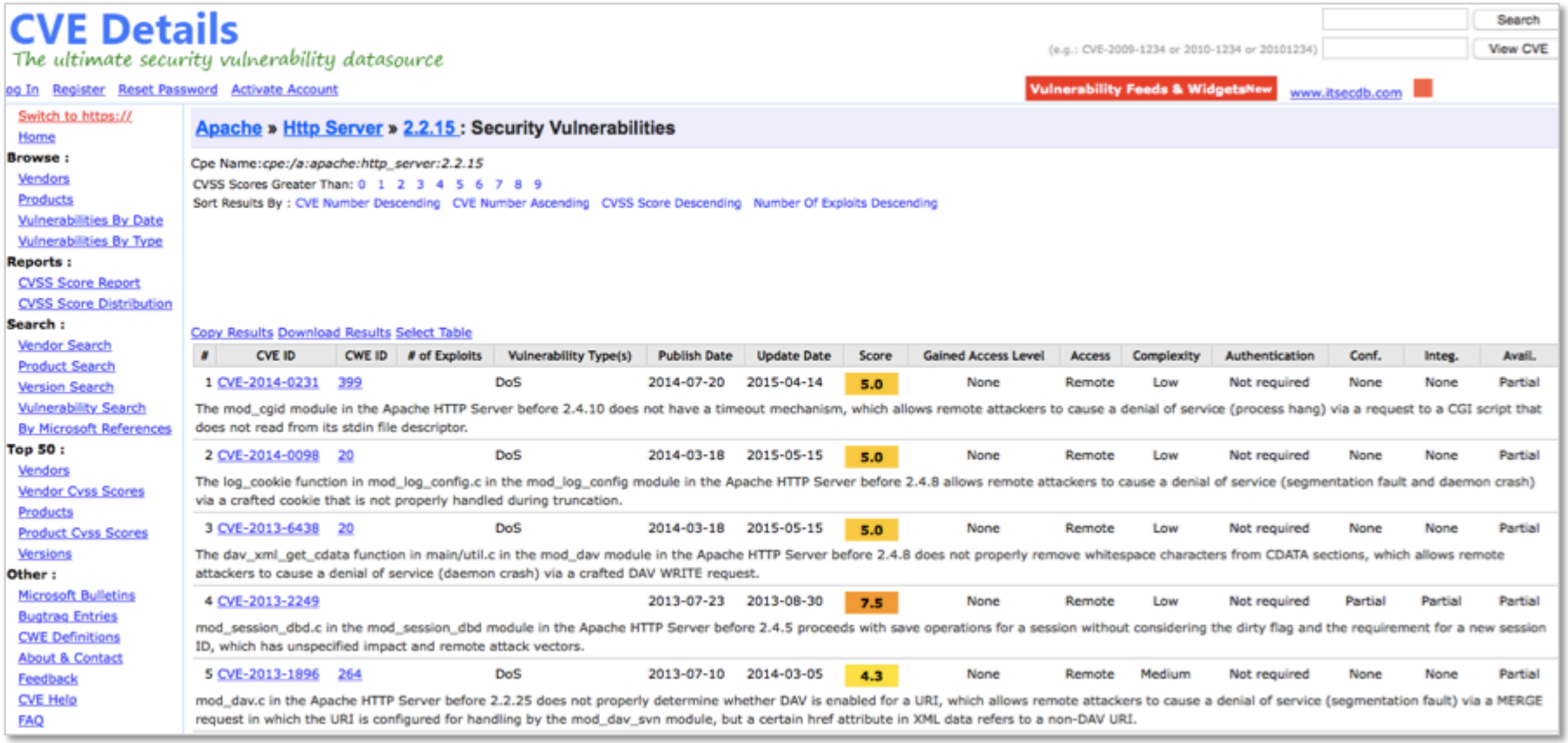
No.	概要	Level
N1	脆弱性が存在するApache(2.2.15)	3
N2	脆弱性が存在するPHP(5.3.3)	3
N3	HTTPヘッダによるバージョン表示	1
N4	推奨しないHTTPメソッドの許可	1
N5	PHP Creditsの表示	1

N1. 脆弱性が存在するApache(2.2.15) (Lv.3)

- 内容
  - Apache 2.2.15 には既知の脆弱性（DoS、XSSなど）が多数存在
- 対策
  - 新しいバージョンに更新
    - Apache 2.2系は 2.2.31 が最新版

N1. 脆弱性が存在するApache(2.2.15) (Lv.3)

http://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-93077/Apache-Http-Server-2.2.15.html



CVE Details

The ultimate security vulnerability datasource

Search | View CVE (e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

og In | Register | Reset Password | Activate Account

Vulnerability Feeds & WidgetsNew | www.itsecdb.com

Switch to https://

Home

Browse :

Vendors

Products

Vulnerabilities By Date

Vulnerabilities By Type

Reports :

CVSS Score Report

CVSS Score Distribution

Search :

Vendor Search

Product Search

Version Search

Vulnerability Search

By Microsoft References

Top 50 :

Vendors

Vendor Cvss Scores

Products

Product Cvss Scores

Versions

Other :

Microsoft Bulletins

Bugtraq Entries

CWE Definitions

About & Contact

Feedback

CVE Help

FAQ

Apache » Http Server » 2.2.15 : Security Vulnerabilities

Cpe Name:*cpe:/a:apache:http_server:2.2.15*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending | CVE Number Ascending | CVSS Score Descending | Number Of Exploits Descending

Copy Results | Download Results | Select Table

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2014-0231	399		DoS	2014-07-20	2015-04-14	5.0	None	Remote	Low	Not required	None	None	Partial

The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.

2	CVE-2014-0098	20		DoS	2014-03-18	2015-05-15	5.0	None	Remote	Low	Not required	None	None	Partial

The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

3	CVE-2013-6438	20		DoS	2014-03-18	2015-05-15	5.0	None	Remote	Low	Not required	None	None	Partial

The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

4	CVE-2013-2249				2013-07-23	2013-08-30	7.5	None	Remote	Low	Not required	Partial	Partial	Partial

mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.

5	CVE-2013-1896	264		DoS	2013-07-10	2014-03-05	4.3	None	Remote	Medium	Not required	None	None	Partial

mod_dav.c in the Apache HTTP Server before 2.2.25 does not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data refers to a non-DAV URI.

脆弱性の識別と評価

- **CVE**
  - Common Vulnerabilities and Exposures
  - 共通脆弱性識別子
  - 脆弱性につける**識別子**
- **CVSS**
  - Common Vulnerability Scoring System
  - 共通脆弱性評価システム
  - **深刻度**を定量的に評価（0～10点）

N1. 脆弱性が存在するApache(2.2.15) (Lv.3)

- 参考
  - http://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-93077/Apache-Http-Server-2.2.15.html
  - CVE番号（CVSSスコア）
    - **CVE-2011-3192 (7.8)**
    - **CVE-2013-2249 (7.5)**
    - CVE-2012-0883 (6.9)
    - 他多数

N2. 脆弱性が存在するPHP(5.3.3) (Lv.3)

- 内容
  - PHP 5.3.3 には既知の脆弱性（バッファオーバーフロー、DoS、XSSなど）が多数存在
- 対策
  - 新しいバージョンに更新
    - 5.3系は 5.3.29でサポート終了（2014年8月14日）
    - 5.4、5.5、5.6系に移行

N2. 脆弱性が存在するPHP(5.3.3) (Lv.3)

- 参考
  - http://www.cvedetails.com/vulnerability-list.php?vendor_id=74&product_id=128&version_id=97802
  - CVE番号（CVSSスコア）
    - **CVE-2012-2688 (10.0)**
    - **CVE-2011-3268 (10.0)**
    - CVE-2011-1092 (7.5)
    - 他多数

N3. HTTPヘッダによるバージョン表示 (Lv.1)

- 発生箇所
  - HTTPレスポンスヘッダ
- 原因
  - サーバ側ソフトウェアの設定不備
- 影響
  - 利用ソフトウェア名やバージョン番号より、存在する脆弱性を特定、不用意な攻撃を招く

N3. HTTPヘッダによるバージョン表示 (Lv.1)

- 確認手順
  - http://api.sandbag2015.net/score/ranking/ へのGET, POSTのレスポンスヘッダ

    Server: Apache/2.2.15 (CentOS)

    X-Powered-By: PHP/5.3.3
- 対策
  - Apache、PHPなどの設定ファイルを適切に設定

N3. HTTPヘッダによるバージョン表示 (Lv.1)

- 修正例
  - httpd.conf

    ServerSignature Off

    ServerTokens ProductOnly
    - Server: Apache~~/2.2.15 (CentOS)~~
  - php.ini

    expose_php=off
    - ~~X-Powered-By: PHP/5.3.3~~

N4. 推奨しないHTTPメソッドの許可 (Lv.1)

- 内容
  - TRACEメソッドが有効
- 原因
  - サーバ側ソフトウェアの設定不備
- 影響
  - 特に考えられないが、不必要なメソッドは無効に
    - TRACEメソッドを悪用する攻撃（XST:Cross-Site Tracing）は、ブラウザ側で対策され影響を受けなくなった

N4. 推奨しないHTTPメソッドの許可 (Lv.1)

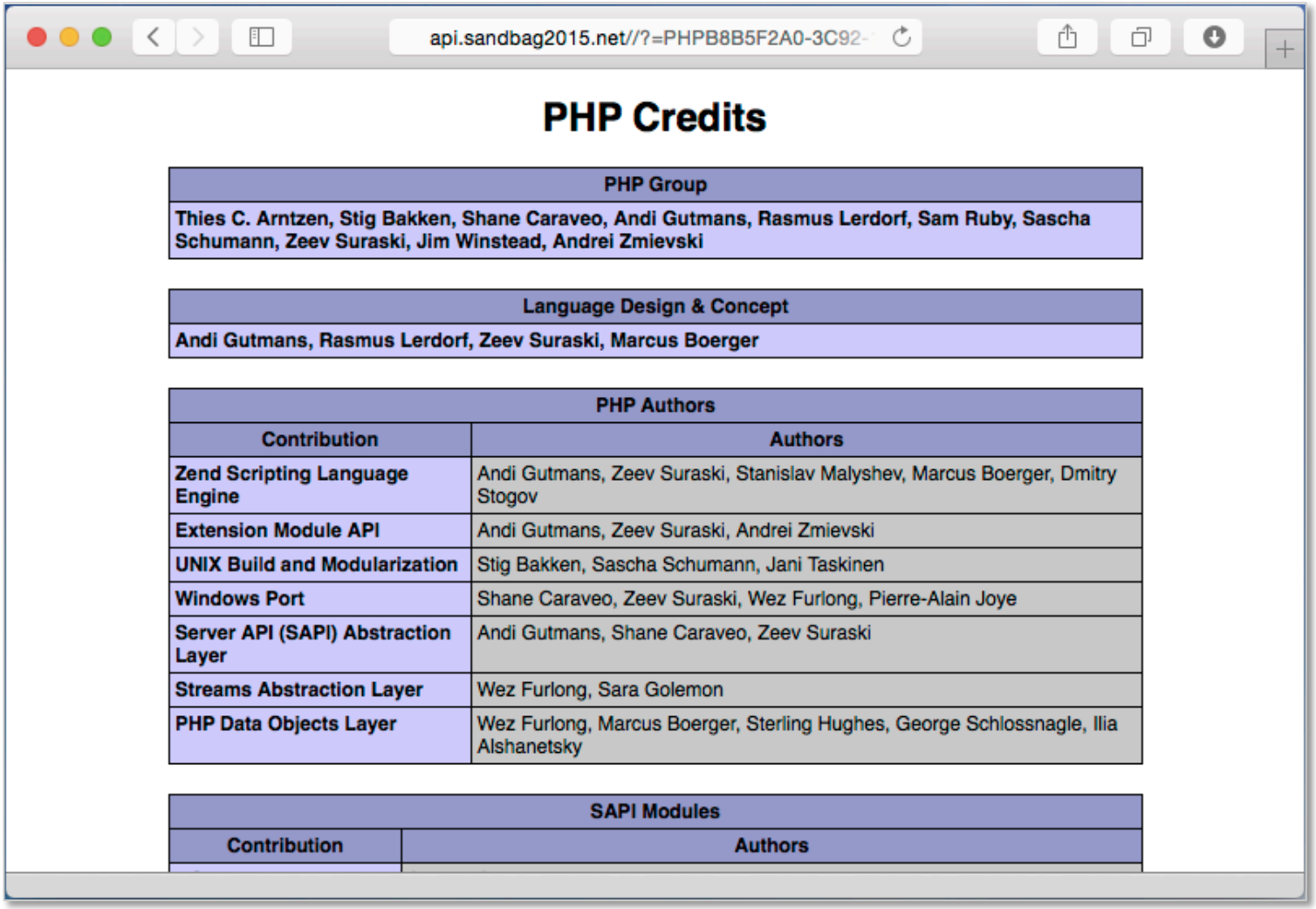
- 対策
  - 設定ファイルを修正

  - httpd.conf
    TraceEnable off

N5. PHP Creditsの表示 (Lv.1)

- 発生箇所
  - http://api.sandbag2015.net//?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
- 原因
  - サーバ側ソフトウェアの設定不備
- 影響
  - PHP Creditsの表示内容から利用バージョンを推測

N5. PHP Creditsの表示 (Lv.1)



N5. PHP Creditsの表示 (Lv.1)

- 対策
  - 設定ファイルを修正

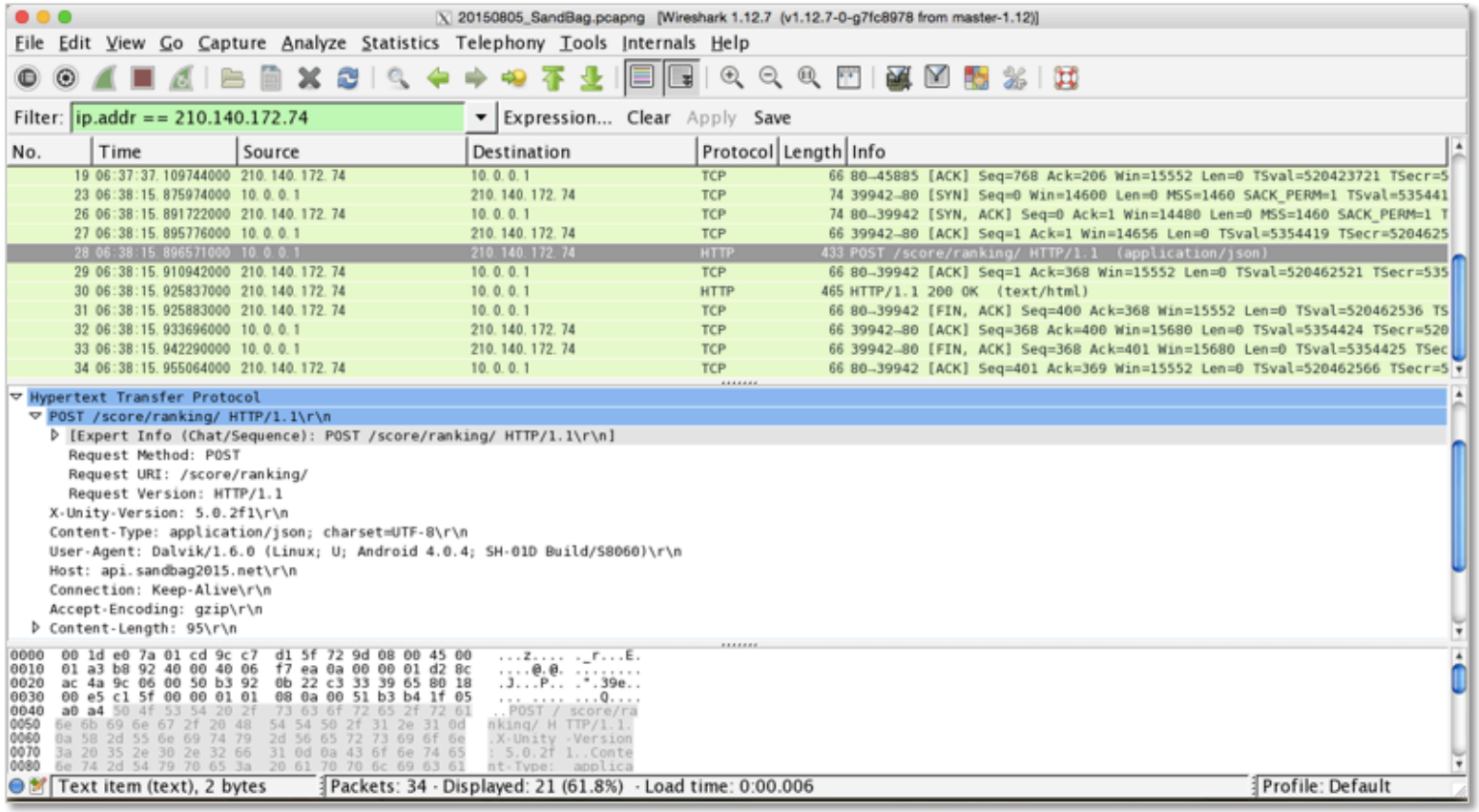
  - php.ini
    expose_php = off

検査ツール

Wireshark	パケットキャプチャ、プロトコルアナライザ
nmap	ポートスキャナ
nikto	HTTPサービスのスキャナ
OWASP ZAP	ブラウザ・アプリ～サーバの通信内容確認、脆弱性検査
sqlmap	SQLインジェクションの調査

Wireshark

- 流れているパケットをキャプチャ、様々なプロトコルを見易く表示



nmap

- 開いているポートを調べる
- 利用サービス名やバージョンを調べる
- 操作例
  - $ nmap IPアドレス
    - 開いているポート番号、一般的なサービス名
  - $ nmap –sV IPアドレス
    - 開いているポート番号、サービス名とバージョン

nmap

```
root@kali:~# nmap -A api.sandbag2015.net

Starting Nmap 6.47 ( http://nmap.org ) at 2015-08-07 17:47 JST
Nmap scan report for api.sandbag2015.net (210.140.172.74)
Host is up (0.016s latency).
rDNS record for 210.140.172.74: 210-140-172-74.jp-east.compute.idcfcloud.com
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.15 ((CentOS))
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Network Distance: 13 hops
 (省略)
OS and Service detection performed. Please report any incorrect results at http://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.69 seconds
```

nikto

- HTTPサービスの脆弱性検査
- 古いソフトウェアの利用、設定の不備、不必要なファイルの公開などを調べる
- 操作例
  - $ nikto –h IPアドレス
    - TCP/80 を調べる
  - $ nikto –h IPアドレス –p ポート番号
    - 指定したポート番号を調べる

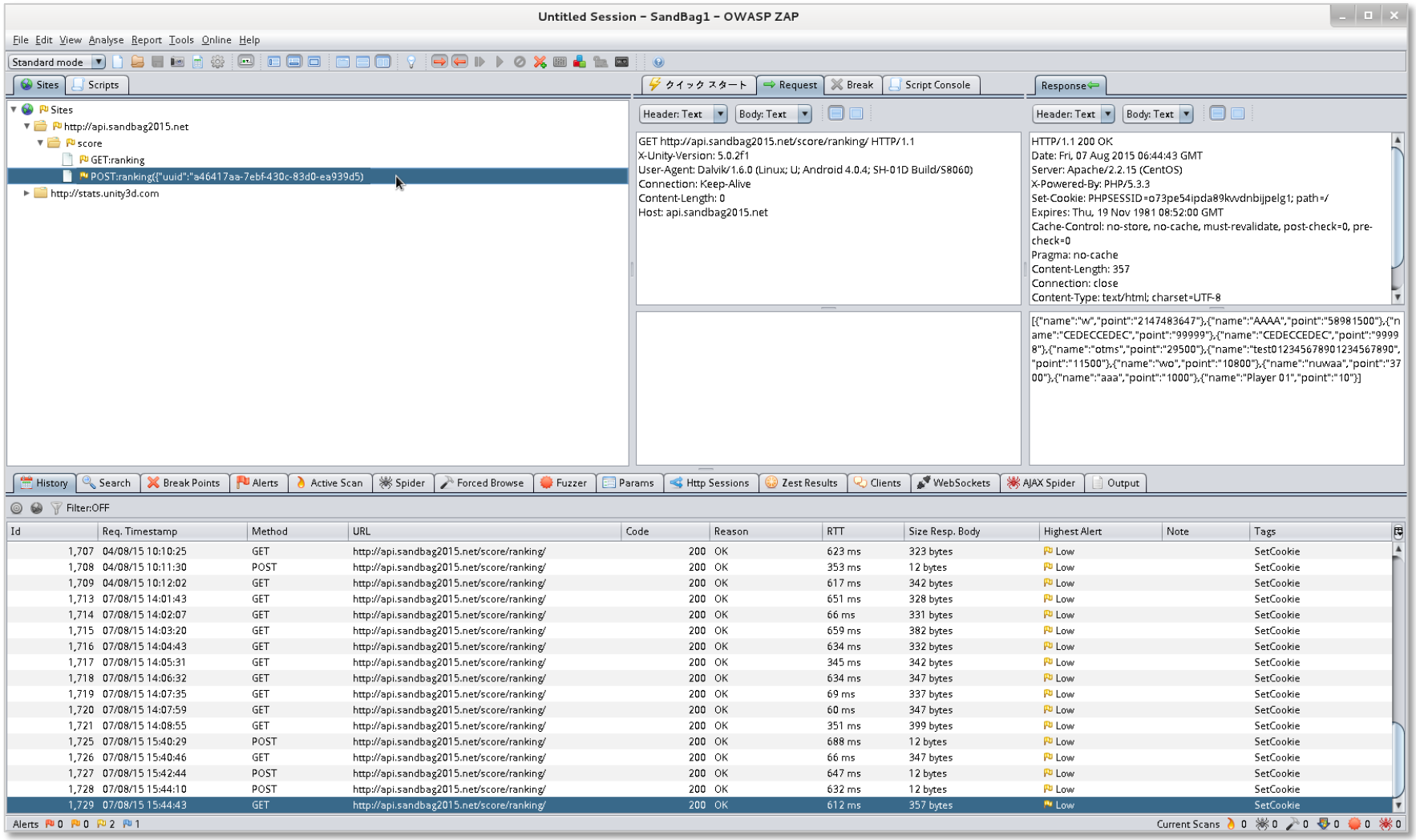
nikto

```
root@kali:~# nikto -h api.sandbag2015.net
- Nikto v2.1.6
 （省略）
+ Server: Apache/2.2.15 (CentOS)
+ Cookie PHPSESSID created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.3.3
+ The anti-clickjacking X-Frame-Options header is not present.
+ Apache/2.2.15 appears to be outdated (current is at least Apache/2.4.7). Apache
2.0.65 (final release) and 2.2.26 are also current.
+ Server leaks inodes via ETags, header found with file /, inode: 263550, size: 8,
mtime: Sun Jun  7 18:18:37 2015
+ Web Server returns a valid response with junk HTTP methods, this may cause false
positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ Uncommon header 'union all select filetoclob('/etc/passwd','server')' found, with
contents: :html,0 FROM sysusers WHERE username=USER --/.html HTTP/1.1 404
+ Uncommon header 'src=javascript' found, with contents: alert('Vulnerable')><Img
Src=¥" HTTP/1.1 404
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially
sensitive information via certain HTTP requests that contain specific QUERY
strings.
 （省略）
```

OWASP ZAP

- ブラウザ・アプリ～サーバの通信内容をキャプチャ
  - HTTPヘッダや通信内容を確認
  - リクエストを一端止め、値を書き換えてサーバに送信
  - レスポンスを一端止め、値を書き換えてブラウザ・アプリに送信
- 自動検査
  - 様々な検査パターン文字列をサーバに送信し、レスポンスから脆弱性の有無を検知

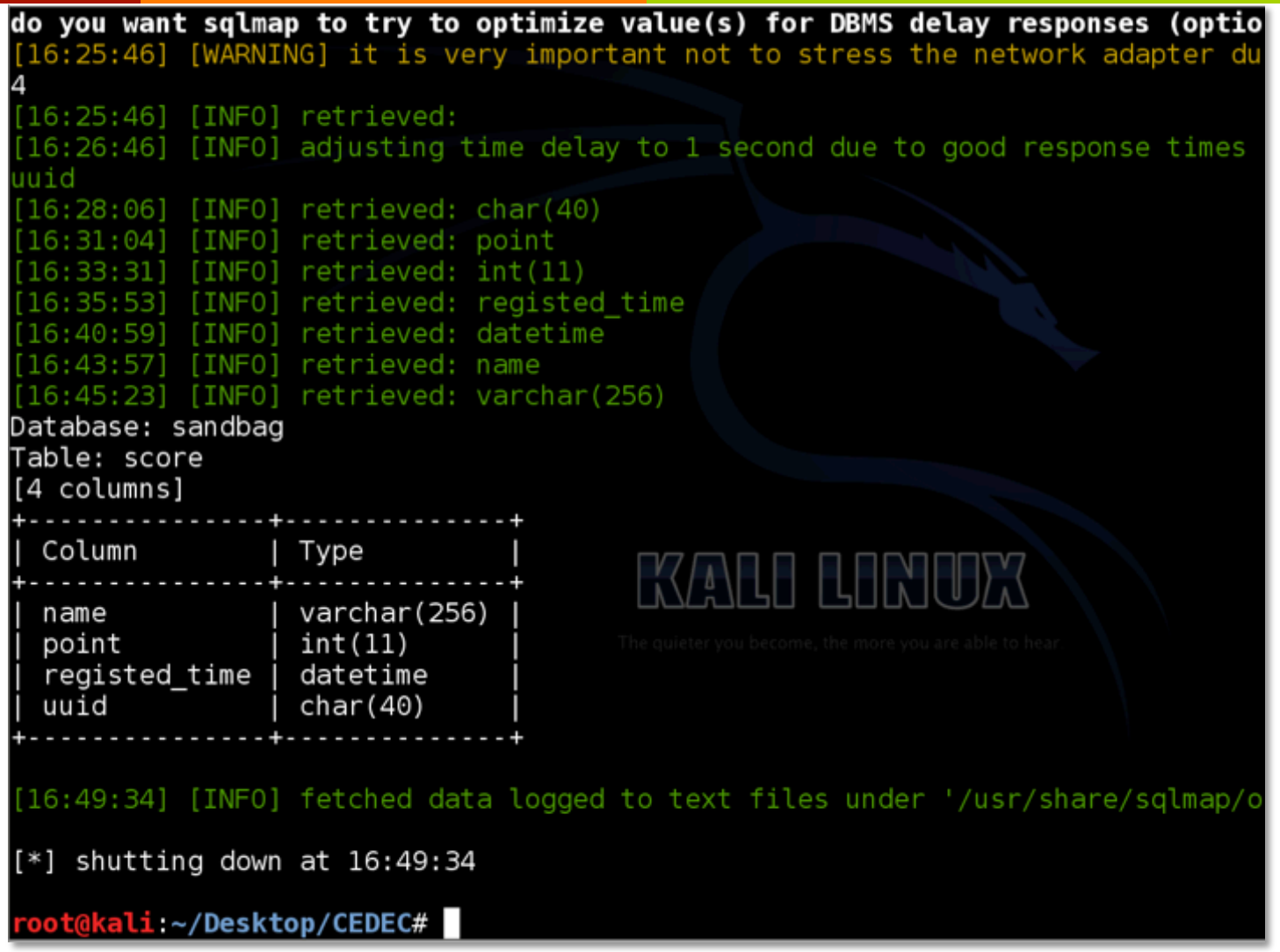
OWASP ZAP


Untitled Session - SandBag1 - OWASP ZAP
File Edit View Analyse Report Tools Online Help
Standard mode
Sites
Scripts
Sites
http://api.sandbag2015.net
score
GET:ranking
POST:ranking({"uuid":"a46417aa-7ebf-430c-83d0-ea939d5}
http://stats.unity3d.com
クイックスタート
Request
Break
Script Console
Response
Header: Text
Body: Text
GET http://api.sandbag2015.net/score/ranking/ HTTP/1.1
X-Unity-Version: 5.0.2f1
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.0.4; SH-01D Build/S8060)
Connection: Keep-Alive
Content-Length: 0
Host: api.sandbag2015.net
HTTP/1.1 200 OK
Date: Fri, 07 Aug 2015 06:44:43 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Set-Cookie: PHPSESSID=o73pe54ipda89kvvdnbijpelg1; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 357
Connection: close
Content-Type: text/html; charset=UTF-8
[{"name":"w","point":"2147483647"},{"name":"AAAA","point":"58981500"},{"name":"CEDECCEDEC","point":"99999"},{"name":"CEDECCEDEC","point":"99998"},{"name":"otms","point":"29500"},{"name":"test01234567890123456789O","point":"11500"},{"name":"wo","point":"10800"},{"name":"nuwaa","point":"3700"},{"name":"aaa","point":"1000"},{"name":"Player 01","point":"10"}]
History
Search
Break Points
Alerts
Active Scan
Spider
Forced Browse
Fuzzer
Params
Http Sessions
Zest Results
Clients
WebSockets
AJAX Spider
Output
Filter:OFF
Id Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
1,707 04/08/15 10:10:25 GET http://api.sandbag2015.net/score/ranking/ 200 OK 623 ms 323 bytes Low SetCookie
1,708 04/08/15 10:11:30 POST http://api.sandbag2015.net/score/ranking/ 200 OK 353 ms 12 bytes Low SetCookie
1,709 04/08/15 10:12:02 GET http://api.sandbag2015.net/score/ranking/ 200 OK 617 ms 342 bytes Low SetCookie
1,713 07/08/15 14:01:43 GET http://api.sandbag2015.net/score/ranking/ 200 OK 651 ms 328 bytes Low SetCookie
1,714 07/08/15 14:02:07 GET http://api.sandbag2015.net/score/ranking/ 200 OK 66 ms 331 bytes Low SetCookie
1,715 07/08/15 14:03:20 GET http://api.sandbag2015.net/score/ranking/ 200 OK 659 ms 382 bytes Low SetCookie
1,716 07/08/15 14:04:43 GET http://api.sandbag2015.net/score/ranking/ 200 OK 634 ms 332 bytes Low SetCookie
1,717 07/08/15 14:05:31 GET http://api.sandbag2015.net/score/ranking/ 200 OK 345 ms 342 bytes Low SetCookie
1,718 07/08/15 14:06:32 GET http://api.sandbag2015.net/score/ranking/ 200 OK 634 ms 347 bytes Low SetCookie
1,719 07/08/15 14:07:35 GET http://api.sandbag2015.net/score/ranking/ 200 OK 69 ms 337 bytes Low SetCookie
1,720 07/08/15 14:07:59 GET http://api.sandbag2015.net/score/ranking/ 200 OK 60 ms 347 bytes Low SetCookie
1,721 07/08/15 14:08:55 GET http://api.sandbag2015.net/score/ranking/ 200 OK 351 ms 399 bytes Low SetCookie
1,725 07/08/15 15:40:29 POST http://api.sandbag2015.net/score/ranking/ 200 OK 688 ms 12 bytes Low SetCookie
1,726 07/08/15 15:40:46 GET http://api.sandbag2015.net/score/ranking/ 200 OK 66 ms 347 bytes Low SetCookie
1,727 07/08/15 15:42:44 POST http://api.sandbag2015.net/score/ranking/ 200 OK 647 ms 12 bytes Low SetCookie
1,728 07/08/15 15:44:10 POST http://api.sandbag2015.net/score/ranking/ 200 OK 632 ms 12 bytes Low SetCookie
1,729 07/08/15 15:44:43 GET http://api.sandbag2015.net/score/ranking/ 200 OK 612 ms 357 bytes Low SetCookie
Alerts 0 0 2 1
Current Scans 0 0 0 0 0 0

sqlmap

- SQLインジェクションの検査に特化
- 脆弱性が存在すれば…
  - データベース情報の列挙、搾取
    - DBMS、ユーザ・権限、データベース、テーブル、カラム、レコード
  - 便利機能
    - ハッシュ化されたパスワードのデコード
    - バックドアをサーバにアップロード、SQLコマンドやOSコマンドを実行

sqlmap


do you want sqlmap to try to optimize value(s) for DBMS delay responses (optio
[16:25:46] [WARNING] it is very important not to stress the network adapter du
4
[16:25:46] [INFO] retrieved:
[16:26:46] [INFO] adjusting time delay to 1 second due to good response times
uuid
[16:28:06] [INFO] retrieved: char(40)
[16:31:04] [INFO] retrieved: point
[16:33:31] [INFO] retrieved: int(11)
[16:35:53] [INFO] retrieved: registed_time
[16:40:59] [INFO] retrieved: datetime
[16:43:57] [INFO] retrieved: name
[16:45:23] [INFO] retrieved: varchar(256)
Database: sandbag
Table: score
[4 columns]
Column	Type
name	varchar(256)
point	int(11)
registed_time	datetime
uuid	char(40)
[16:49:34] [INFO] fetched data logged to text files under '/usr/share/sqlmap/o
[*] shutting down at 16:49:34
root@kali:~/Desktop/CEDEC#
KALI LINUX
The quieter you become, the more you are able to hear

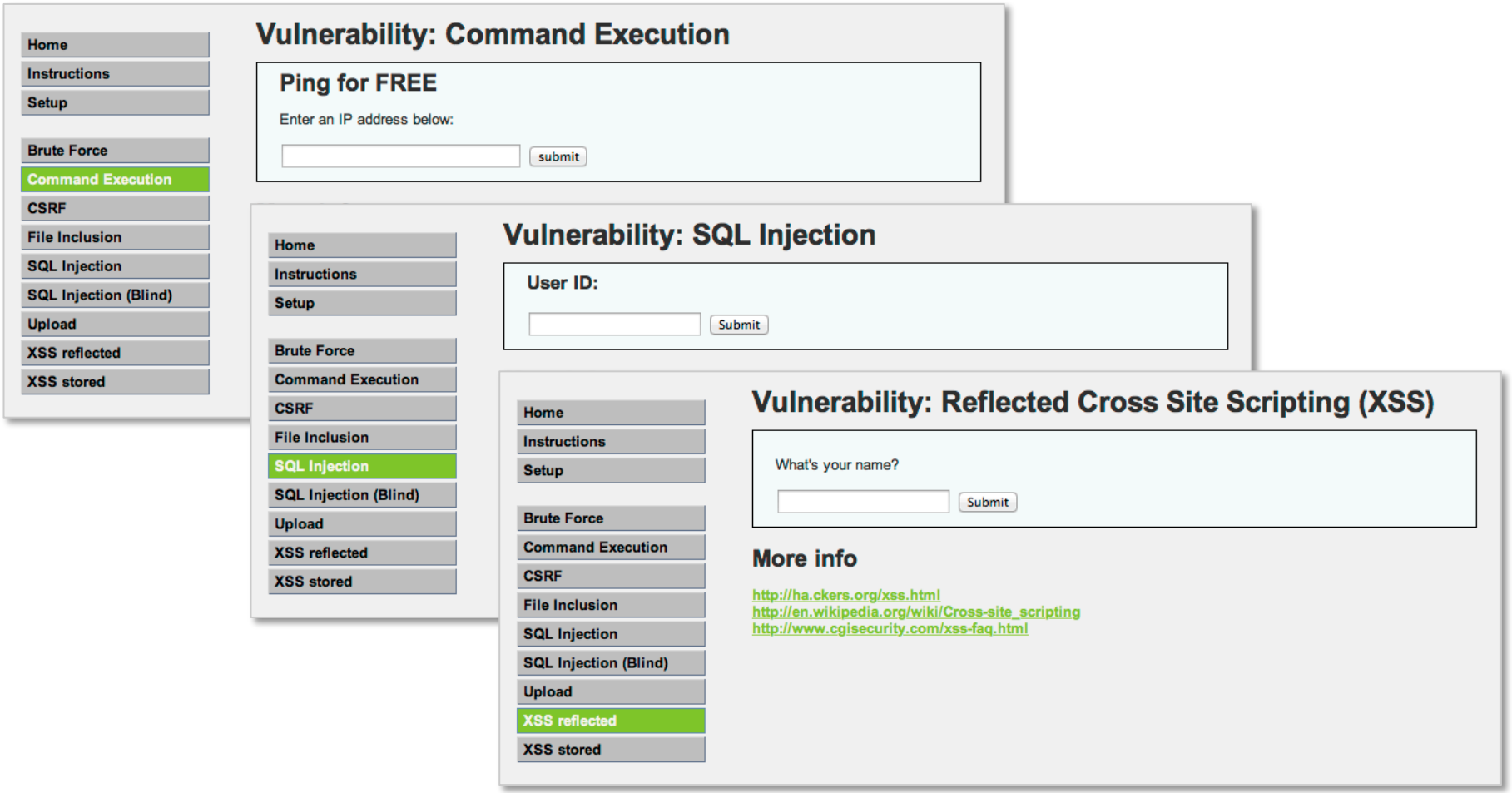
Kali Linux

- セキュリティ診断に特化したLinux
  - 多数の検査ツールがインストール済み
- https://www.kali.org

演習環境：Metasploitable

- 脆弱に作り込まれている教材
  - 古いソフトウェアが多数稼働
  - ダメな設定
  - できの悪いWebアプリケーション
- 配布元
  - http://sourceforge.net/projects/metasploitable/files/Metasploitable2/
  - 仮想環境のゲストOSファイルで配布

Metasploitable



IPA AppGoat

- 脆弱性体験学習ツール
  - IPAが開発・配布（日本語！）
  - Windows上で実行、ブラウザで学習
  - http://www.ipa.go.jp/security/vuln/appgoat/

SECCON 2013

SECCON 2014

- オンライン予選 51位→予選落ち

SECCON 2015

SECCON 2015 開催スケジュール

	日程	開催大会	会場	競技内容
1	2015年8月26日(水)	SECCON 2015 横浜大会	パシフィコ横浜	CEDEC CHALLENGE
2	2015年10月24日(土)	SECCON 2015 広島大会	広島市立大学	熱血シェルコード
3	2015年11月 7日(土)	SECCON 2015 福島大会	会津大学	サイバー甲子園 18才以下 学生限定
4	2015年11月 8日(日)	SECCON 2015 大阪大会	グランフロント大阪	CSIRT演習
5	2015年11月28日(土)	SECCON 2015 九州大会	九州工業大学	Attack & Defense 学生限定
6	12月 5日(土)~6(日)	SECCON 2015 オンライン予選	インターネット	CTF予選(日本語+英語)
7	2016年 1月30日(土)	SECCON 2015 決勝大会 (intercollege)	東京電機大学	CTF決勝戦(日本語) 学生限定
8	2016年 1月31日(日)	SECCON 2015 決勝大会 (international)	東京電機大学	CTF決勝戦(英語)

	日程	開催大会	会場	演習内容
1	2015年 6月 7日(日)	CTF for ビギナーズ 2015 博多	富士通株式会社	Attack & Defense 学生限定
2	2015年 6月14日(日)	CTF for ビギナーズ 2015 札幌	札幌市産業振興センター	Binary, Web, CTF
3	2015年 7月 4日(土)	CTF for ビギナーズ 2015 東京	東京電機大学	Binary, Network, Web, CTF
4	2015年 7月 5日(日)	CTF for ビギナーズ 2015 長野	株式会社電算	Binary, Network, Web, CTF
5	2015年 9月12日(土)	CTF for ビギナーズ 2015 熊本	東海大学	Network, Web, CTF
6	2015年10月 3日(土)	CTF for ビギナーズ 2015 滋賀	立命館大学	Binary, Network, CTF
7	2015年10月 17日(土)	CTF for ビギナーズ 2015 奈良	奈良先端科学技術大	Attack & Defense 学生限定
8	2015年11月 7日(土)	CTF for ビギナーズ 2015 大阪	大阪南港 ATC	CTF in Kansai Open Forum

ありがとうございました

TeamC

（まつもとじゅん）