

الفصل الواحد و العشرين

ثغرة ال Authentication

المؤلف

د.م/ أحمد هاشم الفقي

استشاري أمن المعلومات و التحول الرقمي

Ahmed.Hashem.ElFiky@outlook.com

ثغرة ال Authentication

- يشير مصطلح ثغرة ال Authentication الى هجوم ال Brute-Force والذي يعرف ب عمليات الهجوم بطريقة (التخمين) التي يتم الاعتماد عليها لمحاولة استحصال معلومات معينة كإسم المستخدم وكلمة السر أو الرقم التعريفي الشخصي PIN عن طريقة تخمين مجموعه من الاحتمالات المتوقعة أو إيجاد صفحات أو روابط مواقع الويب مخفية وكذلك إيجاد المفتاح لفك شفرات الرسائل والبيانات. في عملية الهجوم بوساطة ال Brute-Force ، يُستخدم تطبيق مُعد لهذا الغرض بتوليد عدد كبير من كلمات السر التخمينية المتعاقبة بالنسبة لقيمة البيانات المستهدفة. تستخدم الهجمات ب Brute-Force بوساطة المجرمين السبرانيين لكسر حماية البيانات المشفرة وكذلك بوساطة المحللين الامنيين لإختبار مدى أمان شبكات المؤسسات والمنظمات المعنية. وتعتبر هذه الطريقة من أقدم الطرق لكنها مازالت شائعة وفعالة ويستخدمها الكثير من المخترقين.

ثغرة ال Authentication (تكمله...)

- أحد أمثلة ال Brute Force هو هجوم القاموس – Dictionary Attack والذي يقوم بتجربة جميع الاحتمالات التي تتواجد في القاموس لمعرفة كلمة السر. نوع آخر من الهجوم بطريقة التخمين هو إستخدام كلمات السر الشائعة أو توليفة من الأحرف والارقام. هجوم بهذا الشكل أن يستهلك الكثير من الوقت والجهد وكذلك الموارد. لذلك فإن التسمية “ Brute-Force Attack تأتي من قدرة هذا النوع على النجاح بالهجوم بالاعتماد على قوة الحوسبة وعدد التوليفات المستخدمة بدلاً من خوارزميات رياضية بارعة. يأخذ هذا النوع من الهجوم وقتاً من ثواني معدودة الى سنوات كثيرة اعتماداً على طول ودرجة تعقيد كلمة السر التي يقوم المستخدم بإنشائها.

ثغرة ال Authentication (تكمّله...)

- لماذا يتم استخدام ال Brute-Force Attack؟
- تحدث هذه الهجمات عادة في المراحل المبكرة من سلسلة ال Cyber Kill Chain لاسيما في مراحل الاستطلاع والتسلل. يحتاج القراصنة الى تحديد نقاط الولوج لأهدافهم. حالما يحصل المخترقون على صلاحية الولوج للشبكة فإنهم يستخدمون طريقة Brute-Force Attack (التخمين) لترقية إمتيازاتهم في تلك المواقع أو لتشغيل هجمات كسر التشفير. يستعمل المخترقون طريقة ال Brute Force للبحث عن صفحات الويب المخبأة كما أشرنا أعلاه. تتصل صفحات الويب المخبأة بالانترنت لكنها ليست مرتبطة بصفحات أخرى. يمكن لهجوم ال Brute Force Attack اختبار عناوين الويب المختلفة لمعرفة فيما إذا كان إحداها سيعود بصفحة ويب صالحة وسيبحث بالتالي عن تلك الصفحة التي يمكن إستغلالها.

ثغرة ال Authentication (تكملة...)

An example of badly handled *incorrect login* messages is:



Login for user foo: invalid password



Login failed, invalid user ID



Login failed; account disabled



Login failed; this user is not active

All these messages reveal that the provided user is correct.

ثغرة ال Authentication (تكملة...)

The following is an example of how handle the above situation **correctly**:

Login failed; Invalid user ID or password



This does not inform the attacker on which credential is wrong and makes enumeration more difficult.

ثغرة ال Authentication (تكملة...)

The image displays two identical login forms side-by-side, titled "Administration Area Login".

Left Form (Invalid Username):

- Error message: Invalid Username
- Username input: foo
- Password input: masked with dots
- Sign In button
- Need help? link
- Register link
- Cancel button

Right Form (Invalid Password):

- Error message: Invalid Password
- Username input: John
- Password input: masked with dots
- Sign In button
- Need help? link
- Register link
- Cancel button

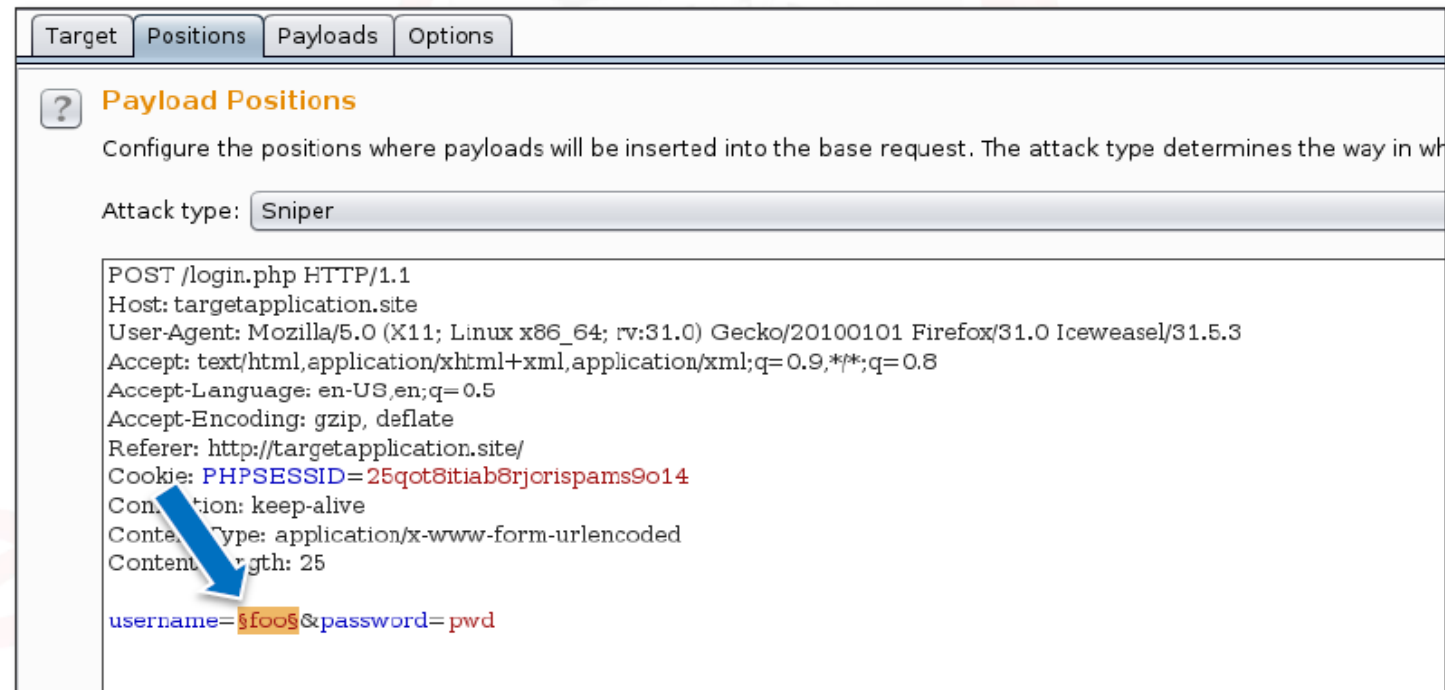
In this example **foo** is an incorrect guess, while **John** is a real username.

ثغرة ال Authentication (تكملة...)

The difference here is easy to find. We receive an explicit *Invalid Username* message when the username is not valid. In contrast, when it is valid we receive an *Invalid Password* message (the passwords can be entered randomly).

ثغرة ال Authentication (تكملة...)

In this example, we want to fuzz the username. So we will add a **position** to the username parameter.



Target Positions Payloads Options

? **Payload Positions**

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

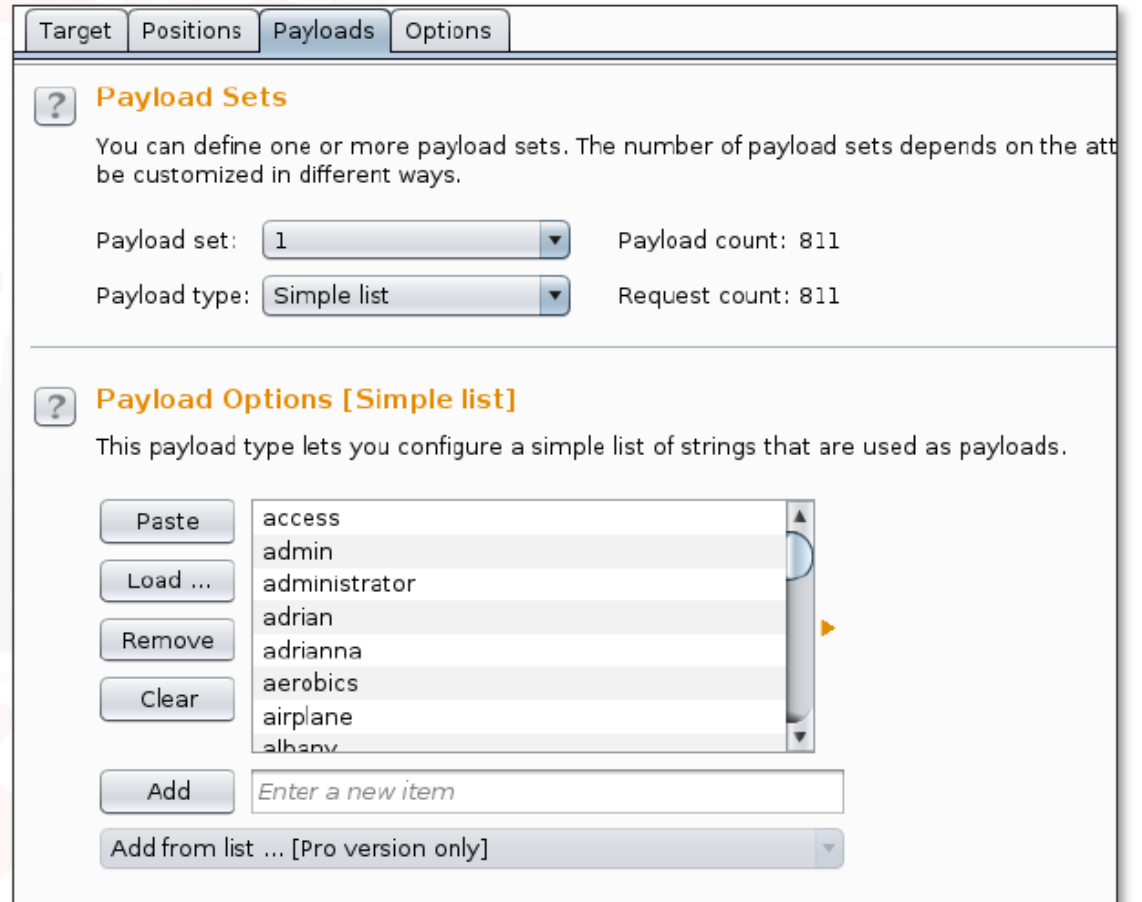
Attack type: **Sniper**

POST /login.php HTTP/1.1
Host: targetapplication.site
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.5.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://targetapplication.site/
Cookie: PHPSESSID=25qot8itiab8rjorisrams9o14
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 25

username=\$foo\$&password=pwd

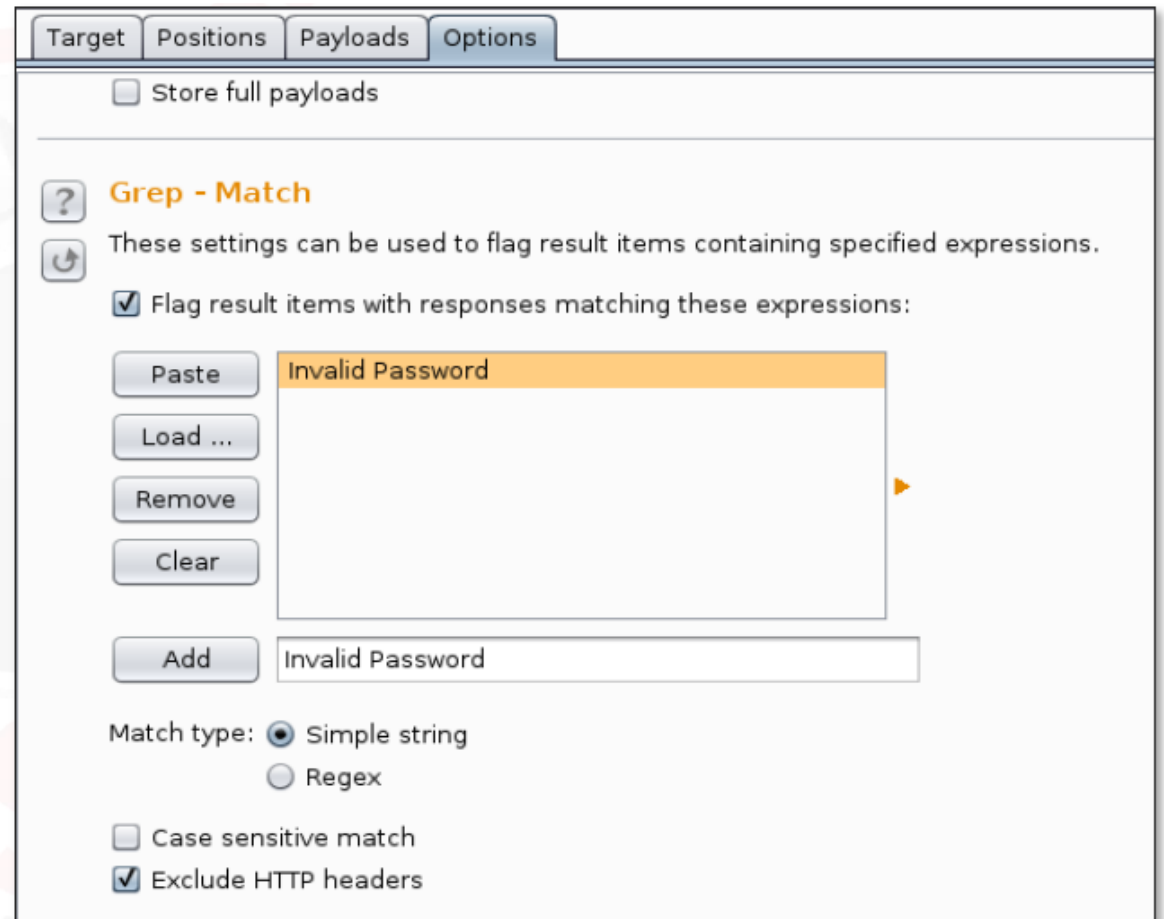
ثغرة ال Authentication (تكملة...)

As you can see, in the **Payload Options** there is a list of common usernames. We used the **Load** button in order to read usernames from a file. Burp automatically reads each line of the file and fills the list.



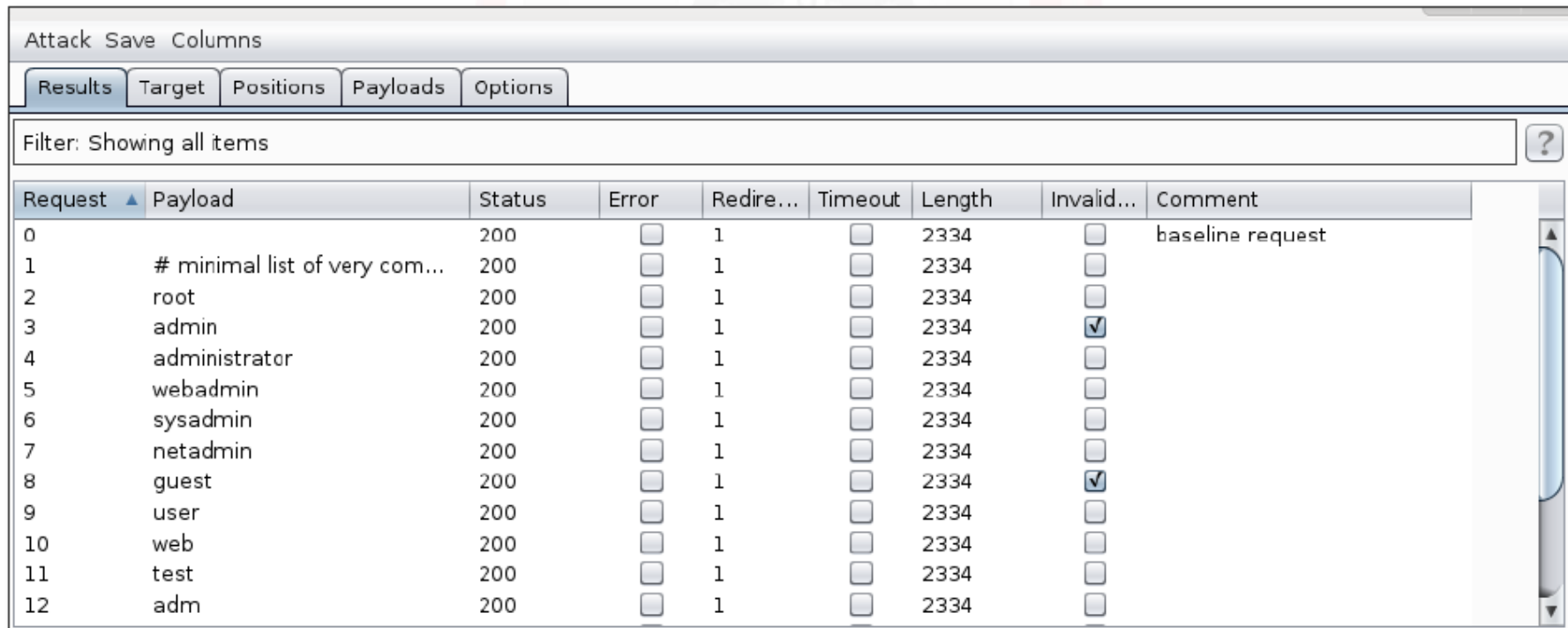
ثغرة ال Authentication (تكملة...)

We are telling Burp to mark a guess as correct, when the text *Invalid password* is found in the web page content.



ثغرة ال Authentication (تكملة...)

As we can see in the results window, two usernames have been enumerated: *admin* and *guest*.



Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Redire...	Timeout	Length	Invalid...	Comment
0		200	<input type="checkbox"/>	1	<input type="checkbox"/>	2334	<input type="checkbox"/>	baseline request
1	# minimal list of very com...	200	<input type="checkbox"/>	1	<input type="checkbox"/>	2334	<input type="checkbox"/>	
2	root	200	<input type="checkbox"/>	1	<input type="checkbox"/>	2334	<input type="checkbox"/>	
3	admin	200	<input type="checkbox"/>	1	<input type="checkbox"/>	2334	<input checked="" type="checkbox"/>	
4	administrator	200	<input type="checkbox"/>	1	<input type="checkbox"/>	2334	<input type="checkbox"/>	
5	webadmin	200	<input type="checkbox"/>	1	<input type="checkbox"/>	2334	<input type="checkbox"/>	
6	sysadmin	200	<input type="checkbox"/>	1	<input type="checkbox"/>	2334	<input type="checkbox"/>	
7	netadmin	200	<input type="checkbox"/>	1	<input type="checkbox"/>	2334	<input type="checkbox"/>	
8	guest	200	<input type="checkbox"/>	1	<input type="checkbox"/>	2334	<input checked="" type="checkbox"/>	
9	user	200	<input type="checkbox"/>	1	<input type="checkbox"/>	2334	<input type="checkbox"/>	
10	web	200	<input type="checkbox"/>	1	<input type="checkbox"/>	2334	<input type="checkbox"/>	
11	test	200	<input type="checkbox"/>	1	<input type="checkbox"/>	2334	<input type="checkbox"/>	
12	adm	200	<input type="checkbox"/>	1	<input type="checkbox"/>	2334	<input type="checkbox"/>	

تم بحمد الله انتهاء الفصل الواحد و العشرين